PRYWATNOŚĆ I ANONIMOWOŚĆ

dla użytkowników komputera i internetu

Im bardziej praca i życie prywatne przenoszą się do internetu i komputerów, tym ważniejsze stają się dla nas prywatność i bezpieczeństwo. Ten cykl poradników pomoże nam o nie zadbać

Zdajemy już sobie dobrze sprawę z tego, jak bardzo każdy użytkownik internetu jest „na widoku" i ile informacji na nasz temat jest zbieranych podczas korzystania z komputera. Jeśli zależy nam na ochronie naszej prywatności, powinniśmy zapoznać się z poradami przedstawionymi w tym kursie oraz zastosować się do nich. Pozwoli nam to kompleksowo zadbać o prywatność i bezpieczeństwo podczas korzystania z komputera i internetu.

Pierwszy odcinek kursu zawiera najważniejsze wskazówki dla użytkowników Windows: jak zmienić ustawienia systemowe i jakich dodatkowych programów warto używać, w kolejnych będziemy poznawać bardziej zaawansowane metody zabezpieczeń.

kd

TEMATY ODCINKÓW KURSU

1. Prywatność i anonimowość w Windows i internecie
2. Anonimowość w internecie dla zaawansowanych
3. Anonimowy system operacyjny

Fot. LisLud/iStockphoto.com

PRYWATNOŚĆ W USTAWIENIACH WINDOWS

Warto znać najważniejsze ustawienia systemu mające znaczenie dla naszej prywatności. Dzięki nim można ograniczyć zbieranie o nas danych przez system, dostosować uprawnienia programów oraz wyłączyć kamerę i mikrofon. Większość omówionych tu opcji znajdziemy w Ustawieniach systemu (można je otworzyć, na przykład klikając prawym przyciskiem myszy na menu Start), w sekcji **Prywatność**.

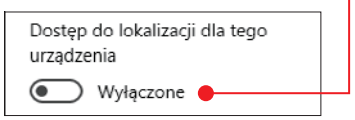
ŚLEDZENIE LOKALIZACJI

Domyślnie Windows 10 na bieżąco zapisuje informacje na temat lokalizacji użytkownika (ma to znaczenie w przypadku użytkowników laptopów). Z jednej strony pozwala to na odnalezienie sprzętu, z drugiej jednak służy do dostosowywania wyświetlanych nam reklam, które są dopasowane do miejsca naszego pobytu. Możemy łatwo wyłączyć śledzenie naszej lokalizacji.

1 Uruchamiamy **Ustawienia systemowe**.

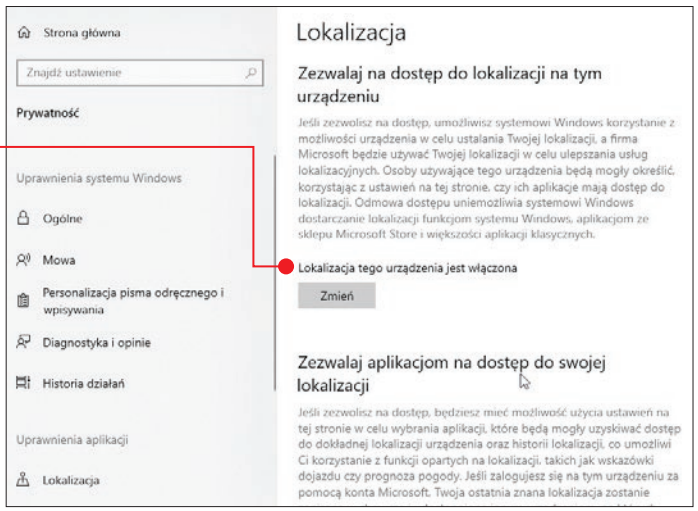
2 Następnie klikamy na pozycję **Prywatność**.

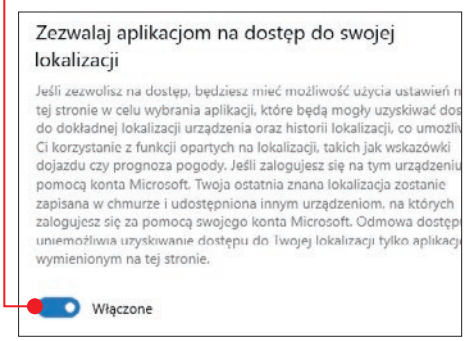
3 Teraz po lewej stronie klikamy na **Lokalizacja**, a po prawej na **Zmień** i zmieniamy opcję dostępu na **Wyłączona**.

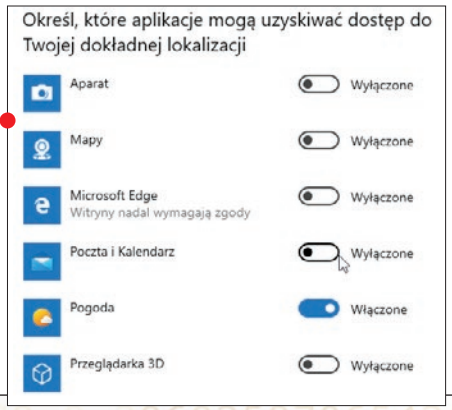


4 Jeśli z różnych względów nie chcemy całkowicie wyłączać opcji lokalizacji, możemy pozostawić ją włączoną i ręcznie kontrolować dostęp wybranych aplikacji do usług lokalizacyjnych. Najpierw musimy zezwolić aplikacjom na dostęp do lokalizacji.

5 Następnie przewijamy widok niżej i ręcznie przyznajemy dostęp do naszej lokalizacji każdej aplikacji lub go blokujemy.

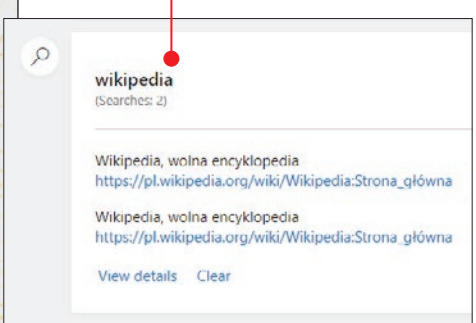


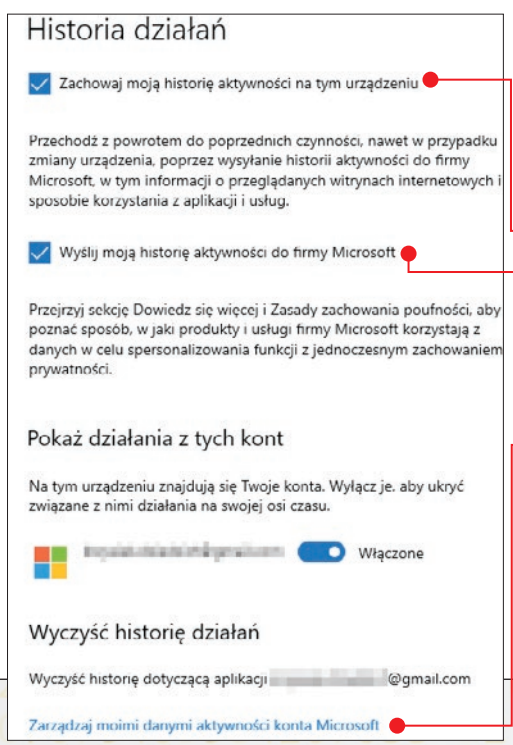




BLOKUJEMY I CZYŚCIMY HISTORIĘ DZIAŁAŃ

Windows od 2018 roku ma niezbyt znaną funkcję **Historia działań**. Pozwala ona na sprawdzanie aktywności użytkownika, jego lokalizacji oraz czynności wykonywanych na komputerze. Dodatkowo łączy informacje z konta użytkownika na różnych urządzeniach, co pozwala na sprawdzenie plików, z którymi pracowaliśmy na innych urządzeniach w przeszłości, czy też historii wyszukiwań.





1 Dostęp do tej funkcji znajdziemy, klikając na **Ustawienia**, **Prywatność**, **Historia działań**.

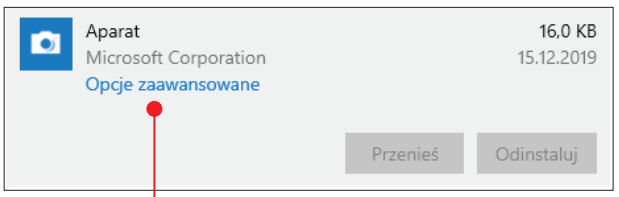
2 Jeśli nie chcemy, aby dane z naszego konta były zbierane i wysyłane, należy wyłączyć opcje zachowywania historii aktywności oraz wysyłania.

3 Następnie musimy jeszcze wyczyścić historię działań. W tym celu klikamy na link w dolnej części ekranu – **Zarządzaj moimi danymi aktywności konta Microsoft**.

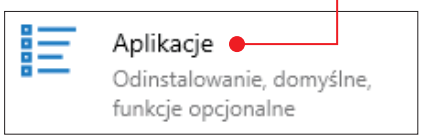
4 Po zalogowaniu się na stronę z danymi dotyczącymi naszego profilu wystarczy przejść przez kolejne kategorie, klikając na opcję **Clear activity** w każdej z osobna.

KONTROLUJEMY UPRAWNIENIA APLIKACJI

Domyślnie system Windows ma aktywowanych wiele uprawnień aplikacji, które mogą naruszać prywatność użytkowników. Warto sprawdzić, które aplikacje mają jakie uprawnienia i wyłączyć te, które mogą naruszyć naszą prywatność.

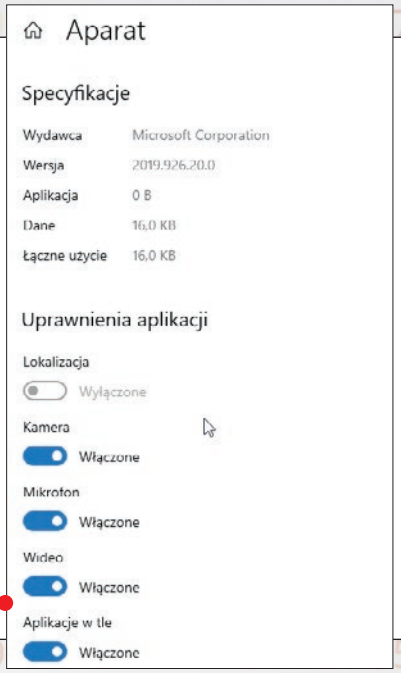


1 Przechodzimy do Ustawień systemu, następnie klikamy na **Aplikacje**.



2 Po prawej stronie na liście wybieramy poszczególne aplikacje i klikamy na **Opcje zaawansowane**. Aplikacje, przy których nie ma linku **Opcje zaawansowane**, nie korzystają z dodatkowych uprawnień w systemie Windows.

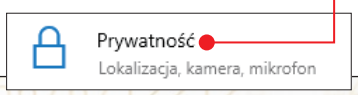
3 W polu **Uprawnienia aplikacji** decydujemy, jakie uprawnienia ma mieć dana aplikacja.



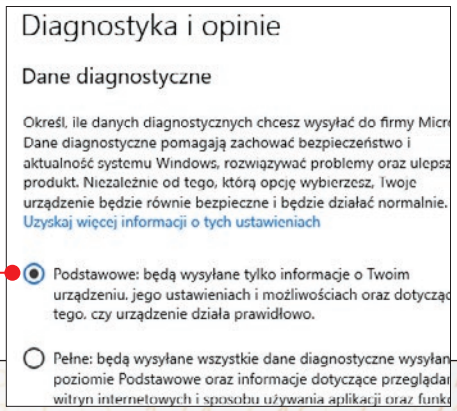
USTAWIENIA ZBIERANIA DANYCH DIAGNOSTYCZNYCH

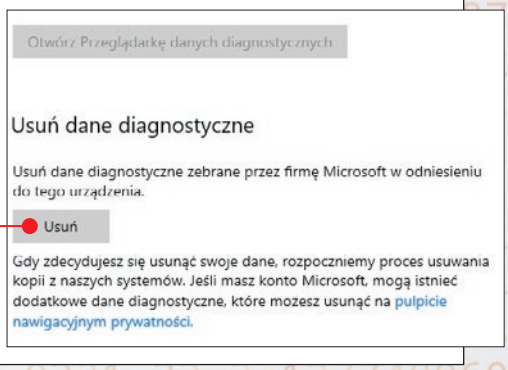
Windows zgodnie z domyślnymi ustawieniami zbiera i wysyła do firmy Microsoft pełne dane diagnostyczne – nie tylko informacje o urządzeniu, jego ustawieniach i możliwościach, ale także dotyczące między innymi przeglądanych witryn, sposobu używania aplikacji i funkcji czy kondycji komputera i wykonywanych na nim działań. Warto ograniczyć poziom zbieranych o nas danych i usunąć te już zapisane. Oto jak to zrobić.

1 Przechodzimy do Ustawień systemu, następnie klikamy na **Prywatność**.



2 Po lewej stronie klikamy na **Diagnostyka i opinie**. Po prawej stronie zaznaczamy **Podstawowe** zamiast **Pełne** i przewijamy widok do pozycji **Usuń dane diagnostyczne**, a potem klikamy na polecenie **Usuń**. Proces usuwania takich danych może potrwać kilka dni.

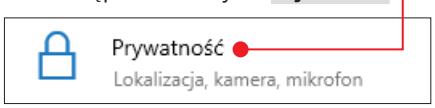




WYŁĄCZAMY DOSTĘP DLA KAMERY I MIKROFONU

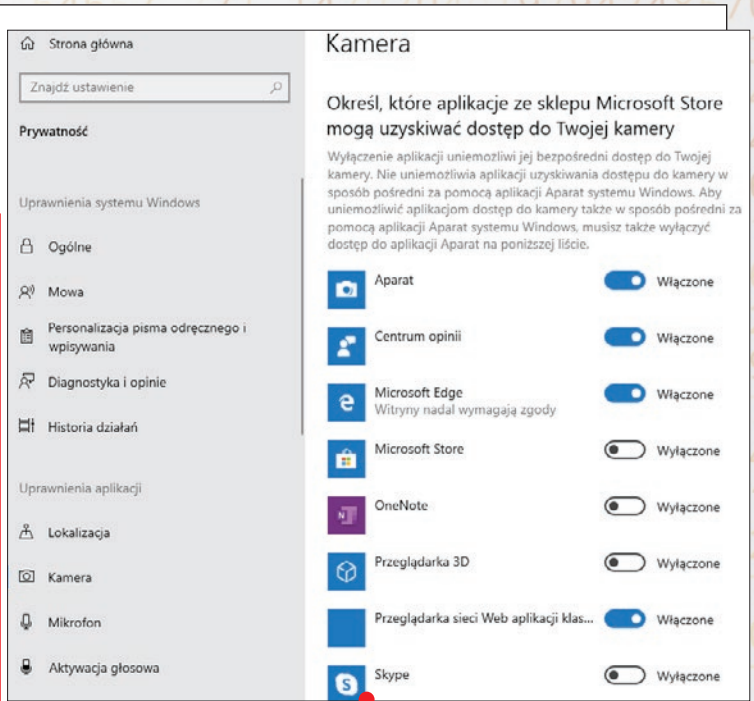
Kluczową rolę dla naszej prywatności mają mikrofon i kamera wbudowane w większość laptopów. Jeśli niebezpieczne aplikacje mają do nich dostęp, może to stanowić zagrożenie, gdyż w czasie rzeczywistym mogą nas nagrywać lub słuchać naszych rozmów, a zapisane dane wysyłać na serwery swoich twórców. Oto jak sprawdzić, jakie aplikacje korzystają z kamery i mikrofonu.

1 Przechodzimy do Ustawień systemu, a następnie klikamy na **Prywatność**.



2 Następnie po lewej stronie klikamy na **Kamera** i przewijamy widok do listy aplikacji. Następnie kontrolujemy każdą aplikację osobno i nadajemy jej odpowiednie uprawnienia. W każdej chwili możemy je zmienić, dlatego też jeśli nie jesteśmy pewni jakiejś aplikacji, najlepiej jest wyłączyć jej dostęp do naszej kamery.

3 Dokładnie te same kroki należy wykonać dla ustawień mikrofonu.

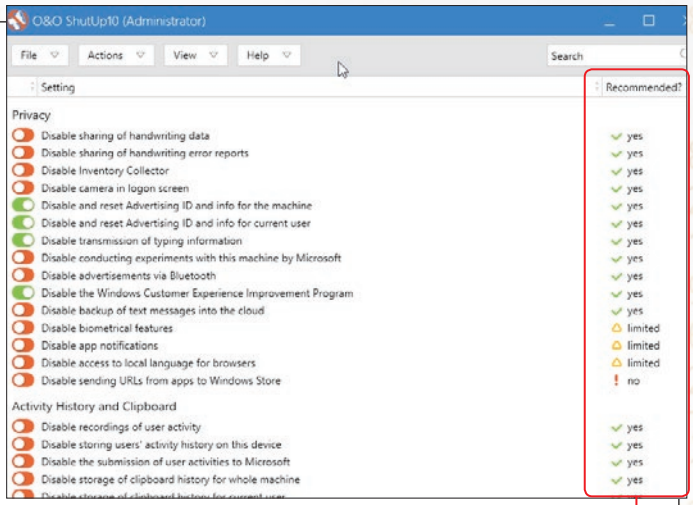


PRYWATNOŚĆ – PROGRAMY POMOCNICZE

Jeśli nie chcemy zmieniać ręcznie ustawień dotyczących prywatności w zakamarkach systemu i nie zniechęca nas konieczność użycia dodatkowych programów, poznajmy dwie najlepsze darmowe aplikacje do tego celu. Pozwalają one na zarządzanie ustawieniami Windows w bardzo przystępny sposób i oferują gotowe profile, które maksymalnie upraszczają cały ten proces.

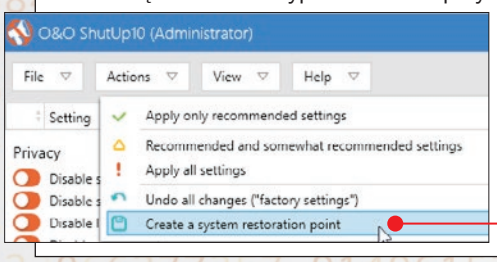
O&O SHUTUP10

O&O ShutUp10 (DVD-KOD: **076**) to program, który pomoże nam zarządzać ustawieniami systemu Windows 10 bez konieczności instalacji na dysku. Do jego poprawnej pracy wymagane są jedynie uprawnienia administratora. Od razu po uruchomieniu będziemy mogli zarządzać wieloma różnymi opcjami. Jest nawet możliwość wyłączenia kamery oraz mikrofonu. Wszystkie funkcje zostały podzielone na specjalne kategorie, dzięki czemu łatwiej jest odnaleźć tę, która nas najbardziej interesuje. Każda opcja w programie ma przypisaną krótką notatkę, która wyjaśnia działanie danej funkcji. Niestety, program nie jest dostępny w polskiej wersji językowej.



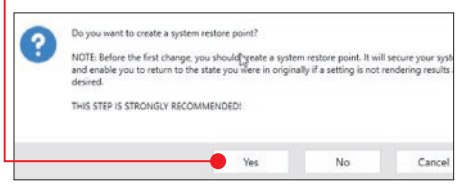
TWORZYMY PUNKT PRZYWRACANIA SYSTEMU

Zanim zaczniemy wprowadzać zmiany w systemie, ważne jest odpowiednie zabezpieczenie się na wszelki wypadek. Punkt przywracania pozwoli nam szybko wrócić do stanu Windows sprzed zmian.



1 Po uruchomieniu programu O&O ShutUp10 klikamy na górnym pasku na **Actions**, a potem na **Create system restoration point**.

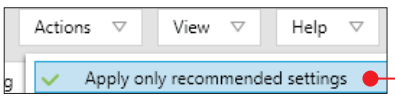
2 Następnie klikamy na **Yes** w celu potwierdzenia chęci wykonania punktu przywracania systemu.



3 Po chwili punkt zostanie utworzony, a my możemy zacząć wprowadzać zmiany bez obaw o stabilną pracę systemu.

WYBIERAMY ZALECANE USTAWIENIA

Po prawej stronie znajduje się kolumna **Recommended?**, a w niej trzy rodzaje domyślnych oznaczeń: zielone **yes**, żółte **limited** i czerwone **no**. Najlepiej jest aktywować opcje oznaczone zielonym **yes** (żeby przełącznik był zielony) – takie ustawienie jest najmniej ryzykowne i obejmuje większość istotnych opcji w systemie.



1 Dlatego na górnym pasku klikamy na **Actions**, **Apply only recommended settings**.

2 Po wprowadzeniu zmian konieczne będzie ponowne uruchomienie systemu w celu ich wprowadzenia.

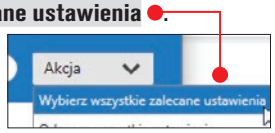
ASHAMPOO ANTISPY

Ashampoo Antispy (DVD-KOD: **014**) to jeden z prostszych programów do kontroli mechanizmów zbierających dane o użytkowniku w systemie Windows 10. W dość niedużym oknie znajdziemy listę z opcjami, które możemy aktywować lub dezaktywować, korzystając ze specjalnego przełącznika po lewej stronie każdej z opcji. Program jest prawie w całości spolszczony, jedynie pojedyncze opisy są w języku angielskim. Funkcje są podzielone na kategorie, dzięki czemu szybko odnajdziemy to, czego szukamy. Do naszej dyspozycji jest również gotowy profil z zalecanymi ustawieniami, które wystarczą do podstawowej ochrony naszych informacji systemowych.

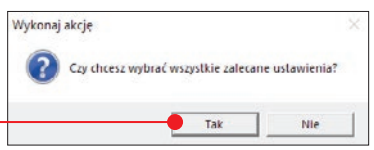
WYBIERAMY ZALECANY PROFIL USTAWIEŃ

Automatycznie po uruchomieniu pojawi się możliwość utworzenia punktu przywracania – warto z niej skorzystać.

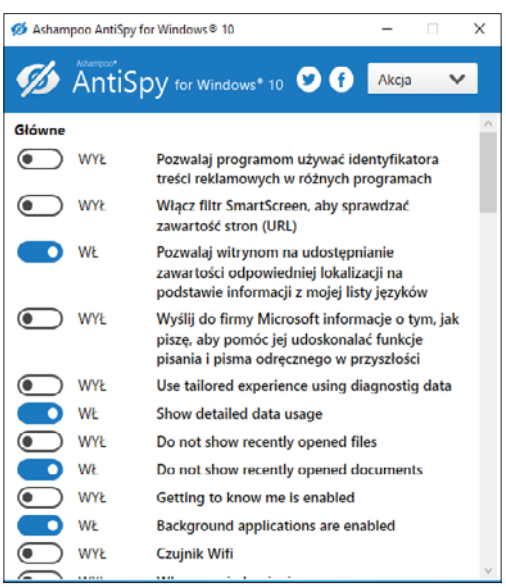
1 Po uruchomieniu programu Ashampoo Antispy klikamy w górnym prawym rogu na **Akcja**, **Wybierz wszystkie zalecane ustawienia**.



2 Pojawi się okno, w którym klikamy na **Tak** w celu potwierdzenia chęci wprowadzenia zmian.



3 Następnie po chwili pojawi się na ekranie informacja o tym, że cały proces został zakończony pomyślnie.



SZYFROWANE POŁĄCZENIE Z INTERNETEM

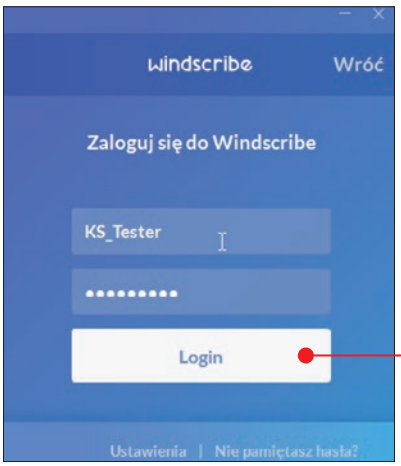
Jeśli musimy skorzystać z internetu w publicznych miejscach poprzez otwarte punkty dostępowe – hotspoty, ryzykujemy, że ktoś może przechwycić nasze dane. Dlatego też bardzo ważne jest odpowiednie zabezpieczenie. Najlepiej jest używać w takich sytuacjach programu typu VPN. Pozwala on na zaszyfrowanie całego ruchu pomiędzy naszym urządzeniem a serwerem końcowym. Dzięki temu w tej wewnętrznej sieci nasz ruch jest całkowicie bezpieczny. Oto jedno z lepszych rozwiązań tego typu w wersji darmowej.

WINDSCRIBE VPN

Bezpłatna wersja programu VPN z pakietem danych 10 GB miesięcznie (po potwierdzeniu adresu e-mail). **Windscribe VPN** (DVD-KOD: **113**) ma prosty, nowoczesny interfejs. Może działać jako program instalowany w Windows, a także jako rozszerzenie do przeglądarki Chrome, Firefox i Opera oraz jako aplikacja mobilna na telefon lub tablet. Program oferuje silne szyfrowanie połączenia z internetem, aby przesyłane przez nas informacje nie mogły być odczytane przez dostawcę usług internetowych ani operatora sieci Wi-Fi. Chroni również naszą prywatność – nie tylko ukrywa nasz adres IP, co pozwala omijać różnego typu internetowe blokady i anonimowo publikować w sieci, ma również funkcje do blokowania trackerów, malware'u i reklam. Do konta użytkownika nie ma przypisanego limitu urządzeń.

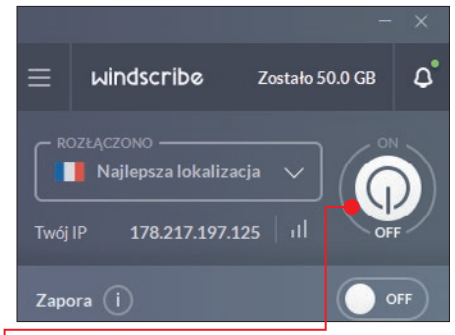
NAWIĄZUJEMY BEZPIECZNE POŁĄCZENIE

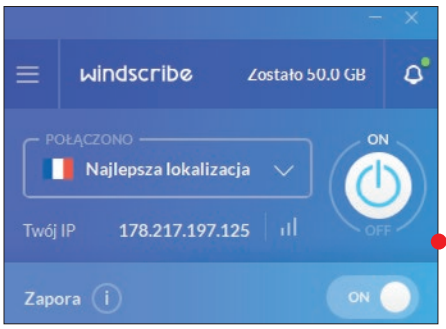
1 Instalujemy Windscribe VPN, uruchamiamy go, zakładamy konto na serwerze programu i klikamy na link potwierdzający w wiadomości e-mail.



2 Następnie możemy zalogować się do programu – po podaniu danych klikamy na **Login**.

3 Teraz wystarczy kliknąć na symbol zasilania, by aktywować połączenie VPN z wybranym serwerem.





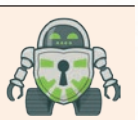
4 Po nawiązaniu bezpiecznego połączenia wygląd okna aplikacji zostanie zmieniony na niebieski.

SZYFROWANIE DYSKU I DANYCH

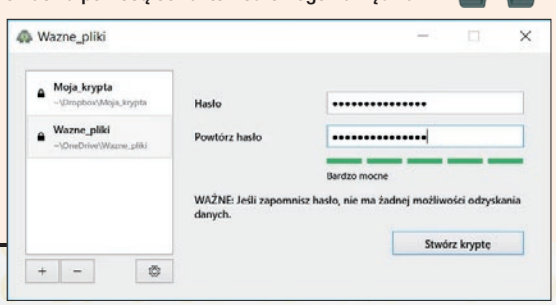
Większość prywatnych danych przechowujemy na dyskach naszych komputerów lub na specjalnych nośnikach zewnętrznych. Jeśli zaszyfrujemy dysk w komputerze, nikt nie będzie mógł uruchomić zainstalowanego na nim systemu bez znajomości odpowiedniego hasła lub użycia odpowiedniego klucza fizycznego. Taka forma ochrony zapewnia całkowite bezpieczeństwo wszystkich danych zapisanych na dysku. Do szyfrowania możemy użyć rozwiązania firmy Microsoft, czyli funkcji **BitLocker**. Jest to systemowe rozwiązanie, które oferowane jest w przypadku Windows 10 użytkownikom wersji Pro, Enterprise i Education. Dzięki tej funkcji systemu Windows można szyfrować całe dyski i partycje. Jeśli nie mamy odpowiedniej edycji systemu lub wolimy rozwiązania Open Source, możemy skorzystać z programu **VeraCrypt**. Oferuje on bezpieczne szyfrowanie i przeszedł różne audyty, które nie wykazały dziur bezpieczeństwa pozwalających na łatwe rozszyfrowywanie danych. Dla większości użytkowników, którzy chcą zaszyfrować cały dysk lub wybraną partycję systemową, najłatwiej będzie skorzystać z wbudowanego w system narzędzia. Jeśli natomiast chcemy zaszyfrować konkretny zasób, folder lub nie mamy wspieranej przez funkcję BitLocker wersji systemu, musimy skorzystać z możliwości szyfrowania programu VeraCrypt. **Uwaga!** Funkcja BitLocker nie jest dostępna dla użytkowników wersji Home.

	BitLocker	VeraCrypt
Dostępność	Windows Pro, Enterprise, Education	Dla każdego
Opcje szyfrowania	Cała partycja	Partycja lub jej część
Kompatybilność przy przenoszeniu nośników	Przy zabezpieczeniu TPM nie możemy przenosić dysku między komputerami	Działa na każdym komputerze z zainstalowanym programem VeraCrypt

Cryptomator: szyfruje dane na dyskach chmurowych

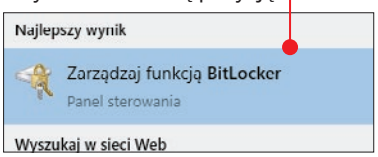


Dane umieszczane na dyskach online, w chmurze – na Dropboxie, Dysku Google lub w innych podobnych usługach, możemy szyfrować za pomocą otwartoźródłowego narzędzia **Cryptomator** (DVD-KOD: **025**). Program szyfruje dane po stronie użytkownika algorytmem AES z 256-bitowym kluczem przed wysłaniem ich do chmury. Pliki i foldery są ukrywane w tak zwanych kryptach, w których zostają ukryte również ich nazwy, rozmiary oraz struktura folderów.

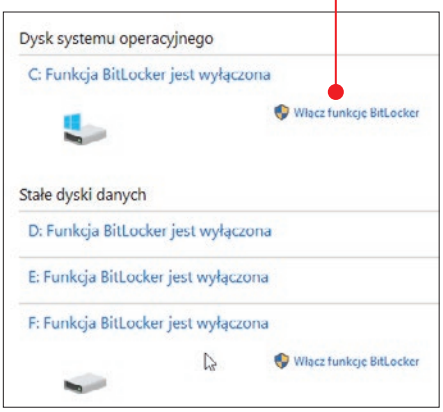


BITLOCKER: SZYFRUJEMY PARTYCJĘ

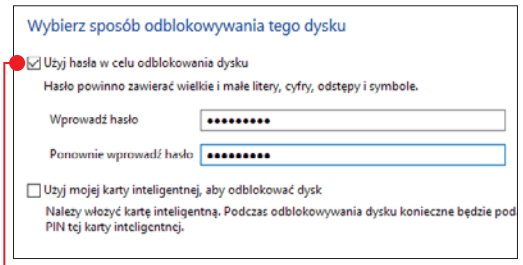
1 W wyszukiwarkę systemu Windows 10 wpisujemy **BitLocker** i klikamy na znalezioną pozycję.



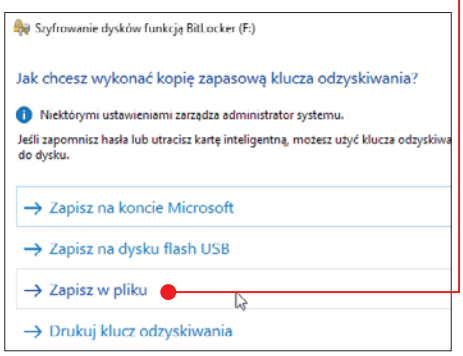
2 Teraz przy partycji, którą chcemy zaszyfrować, klikamy na **Włącz funkcję BitLocker**.



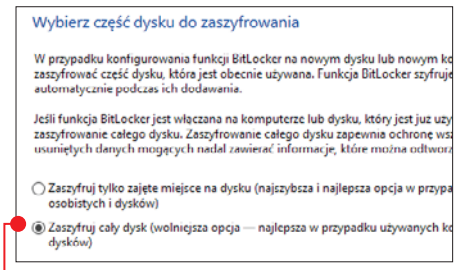
3 Następnie wybieramy opcję **Użyj hasła w celu odblokowania dysku**, podajemy je dwukrotnie i klikamy na **Dalej**.



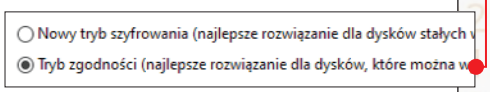
4 Teraz tworzymy kopię zapasową klucza odzyskiwania, klikamy na **Zapisz w pliku** i wybieramy dowolną lokalizację na innej partycji. Klikamy na **Dalej**.



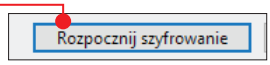
5 Następnie wybieramy opcję **Zaszyfruj cały dysk** – w przypadku gdy nasz dysk był już wykorzystywany przez dłuższy czas – i klikamy na **Dalej**.



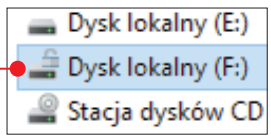
6 Jeśli szyfrujemy dysk, który będzie pracował również ze starszymi systemami, zaleca się wybrać opcję **Tryb zgodności** i przejść **Dalej**.



7 Na koniec klikamy na **Rozpocznij szyfrowanie**.



8 Przy symbolu partycji pojawi się kłódka. Po uruchomieniu komputera przed skorzystaniem z partycji trzeba będzie podać hasło w celu jej odblokowania. Zaszyfrowanie dysku funkcją BitLocker może minimalnie zmniejszyć jego wydajność, ale nie powinno to stanowić problemu w przypadku nowszych dysków HDD i szybkich SSD.



TWORZYMY PRZENOŚNY SEJF Z VERACRYPT

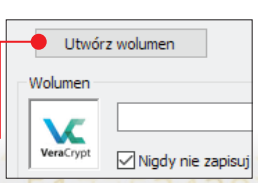
VeraCrypt (DVD-KOD: **108**) to jeden z najlepszych programów do szyfrowania dysków, przenośnych nośników oraz tworzenia bezpiecznych kontenerów na dane. Program ten stworzono na bazie TrueCrypt, który przestał być rozwijany (poprawiono luki bezpieczeństwa, które w nim znaleziono). Szyfrowanie odbywa się przy wykorzystaniu najbezpieczniejszych algorytmów AES-256, Twofish, Serpent i innych. Mimo wykorzystywania silnych algorytmów proces szyfrowania nie trwa długo, a wydajność pracy dysku nie powinna być zauważalnie mniejsza, zwłaszcza jeśli korzystamy z nośnika nowszej generacji.

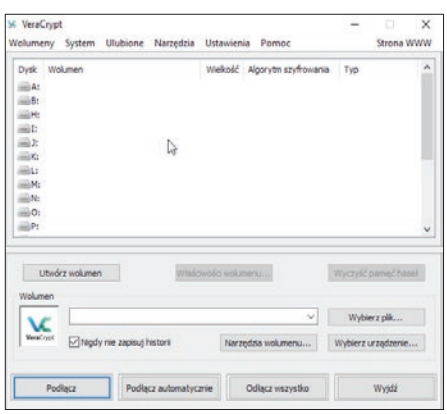
SZYFRUJEMY NOŚNIK USB

Uwaga! Przed rozpoczęciem tego procesu trzeba przenieść wszystkie dane na inny dysk, ponieważ nośnik w trakcie szyfrowania będzie formatowany.

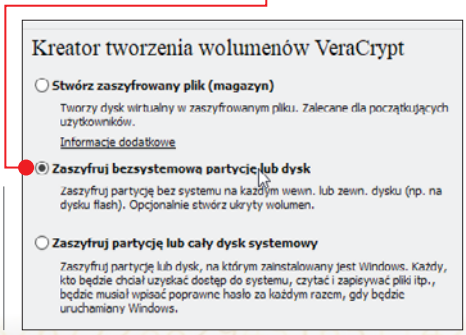
1 Podłączamy wybrany nośnik do naszego komputera i uruchamiamy program VeraCrypt.

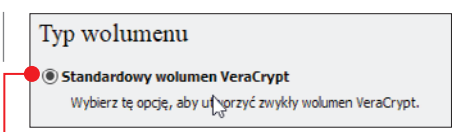
2 Następnie klikamy na przycisk **Utwórz wolumen**.





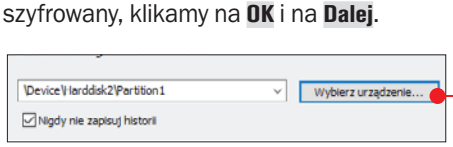
3 Wybieramy opcję **Zaszyfruj bezsystemową partycję lub dysk** i klikamy na **Dalej**.



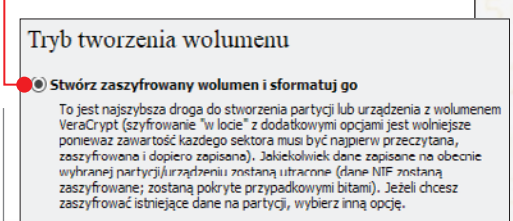


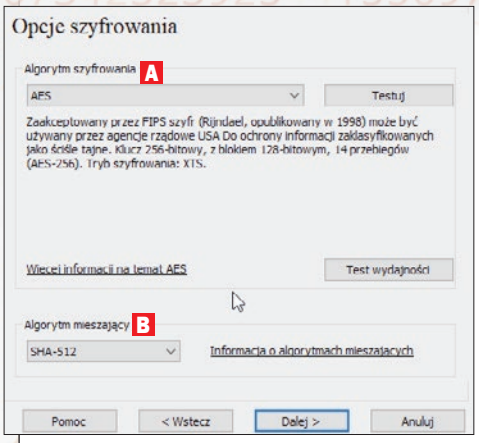
4 Zaznaczamy opcję **Standardowy wolumen VeraCrypt** i przechodzimy **Dalej**.

5 Teraz klikamy na **Wybierz urządzenie**, wskazujemy nośnik, który ma zostać zaszyfrowany, klikamy na **OK** i na **Dalej**.



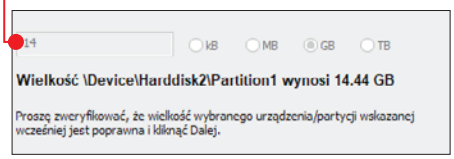
6 Następnie wybieramy pierwszą opcję od góry i klikamy na **Dalej** – po zaznaczeniu tej opcji szyfrowanie nośnika będzie znacznie szybsze.



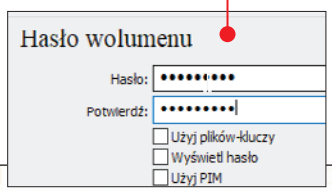


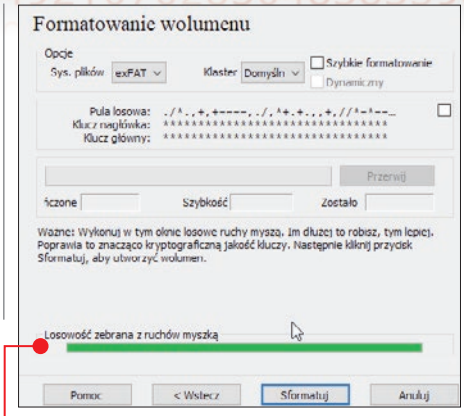
7 Pozostawiamy domyślne ustawienia algorytmów szyfrowania A i mieszającego B i przechodzimy **Dalej**.

8 Weryfikujemy rozmiar nośnika i jeśli jest poprawny, przechodzimy **Dalej**.



9 Teraz podajemy dwukrotnie hasło, które będzie służyć do zabezpieczania naszego nośnika.



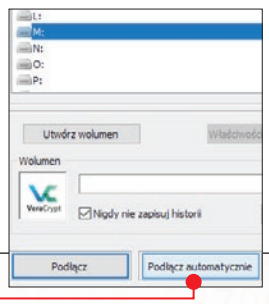


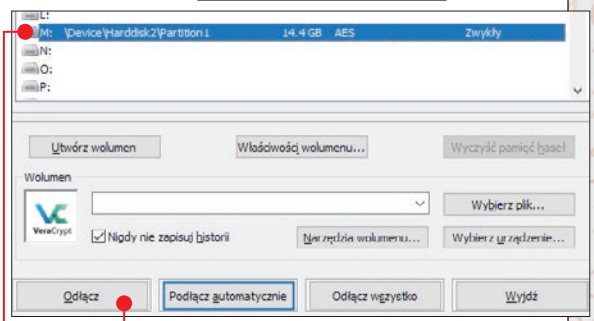
10 Następnie ustalamy system plików, poruszamy myszką aż do momentu, gdy dolny pasek zapełni się na zielono, i klikamy na **Sformatuj**. Na koniec klikamy na przycisk **Wyjście**.

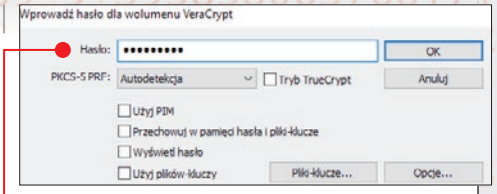
KORZYSTAMY Z ZASZYFROWANEGO NOŚNIKA

1 Po podłączeniu zaszyfrowanego nośnika do komputera z Windows pojawi się komunikat o formatowaniu, klikamy na **Anuluj**.

2 Uruchamiamy VeraCrypt, z okna na górze wybieramy nieużywaną literę dysku i klikamy na **Podłącz automatycznie**.

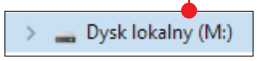






3 Następnie podajemy hasło i klikamy na **OK**.

4 Po zakończeniu montowania nośnika możemy z niego korzystać jak z normalnego dysku i uzyskamy do niego dostęp na przykład poprzez Eksplorator.



5 Zanim zakończymy pracę z zaszyfrowanym nośnikiem, w oknie programu VeraCrypt wybieramy dany wolumen i klikamy na **Odłącz**. Dopiero po odmontowaniu możemy bezpiecznie odłączyć nasz nośnik. W innym przypadku ryzykujemy uszkodzenie naszego sejfu.

ZABEZPIECZENIA PRZEGLĄDARKI

Do popularnych przeglądarek, takich jak Google Chrome, Mozilla Firefox czy Opera, możemy dodać specjalne rozszerzenia, które zwiększają bezpieczeństwo oraz chronią przed potencjalnymi zagrożeniami. Oto jak to zrobić i na jakie rozszerzenia zwrócić uwagę.

CHROME

Zobaczmy, jak dodawać rozszerzenia w najpopularniejszej w Polsce przeglądarce Google Chrome.

INSTALUJEMY ROZSZERZENIA

W oknie Chrome musimy kliknąć na trzy kropki w prawym górnym rogu, a następnie przesunąć kursor na **Więcej narzędzi** i kliknąć na **Rozszerzenia**. Po lewej stronie ekranu klikamy na trzy kreski i na samym dole wybieramy opcję **Otwórz Chrome Web Store**. Teraz możemy skorzystać z pola wyszukiwania dodatków. Po kliknięciu na wybrany dodatek wystarczy jeszcze tylko kliknąć na **Dodaj do Chrome**, a po chwili pokaże się okno z prośbą o potwierdzenie. Po potwierdzeniu dodatek zostanie zainstalowany.

FIREFOX

Firefox to lubiana przeglądarka z rozbudowanym trybem prywatnym z ochroną przed śledzeniem. Jest znany z tego, że jego możliwości można rozbudowywać dzięki dodatkom.

INSTALUJEMY ROZSZERZENIA

Po uruchomieniu Firefoxa klikamy w prawym górnym rogu okna na trzy kreski i z listy wybieramy opcję **Dodatki**.
Następnie po lewej stronie klikamy na **Pobierz dodatki**, a po prawej na **Znajdź więcej dodatków**. Korzystając z pola wyszukiwania, znajdujemy potrzebny nam dodatek. Po wybraniu dodatku klikamy na **Dodaj do Firefoxa**, a po chwili przyznajemy uprawnienia, klikając na **Dodaj**.

OPERA

Opera to warta uwagi przeglądarka z ciekawymi autorskimi usprawnieniami. Ma między innymi wbudowaną blokadę reklam i darmowy VPN.

INSTALUJEMY ROZSZERZENIA

W oknie przeglądarki klikamy w lewym górnym rogu na **Menu**, przesuwamy kursor na **Rozszerzenia i** klikamy na **Pobierz rozszerzenia**. Wpisujemy w pole wyszukiwania nazwę dodatku lub wyszukujemy go w katalogu ogólnym. Jeśli zdecydujemy się go dodać, klikamy na zielony przycisk **Dodaj do Opery**. Instalacja przebiega automatycznie i nie musimy już nic potwierdzać. W celu skorzystania z dodatku wystarczy kliknąć na jego ikonę po prawej stronie paska adresowego.

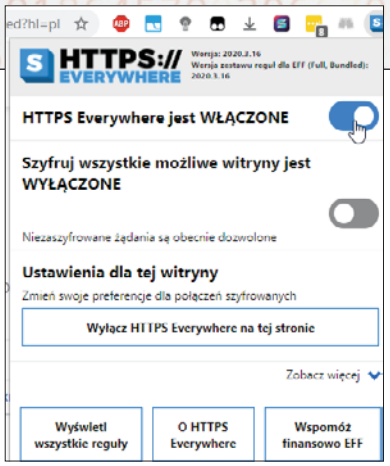
HTTPS EVERYWHERE

Jest to bardzo prosty dodatek, który pomoże poprawić nasze bezpieczeństwo w sieci. Często witryny mogą mieć zaszyfrowaną tylko stronę główną, podczas gdy domyślnie podstrony będą wczytywały się jako zwykłe HTTP bez możliwości ochrony danych, które odbieramy i wysyłamy. Dodatek wymusza stosowanie protokołu HTTPS, jeśli tylko dana domena na to pozwala. (Zawsze sprawdzajmy, korzystając z poczty lub bankowości internetowej, czy jesteśmy połączeni protokołem HTTPS).

KORZYSTANIE Z DODATKU

1 Przy pierwszym uruchomieniu zostaniemy zapytani, czy chcemy korzystać z usług **SSL Observatory**. Jest to usługa, która pomaga wykryć, czy nasza przeglądarka nie została zaatakowana. Wystarczy kliknąć na **Tak**.

2 Upewniamy się, czy funkcja **HTTPS Everywhere** jest włączona. Teraz w trakcie przeglądania witryn automatycznie wszelkie odnośniki, na które możemy kliknąć, będą uruchamiane przez protokół HTTPS, jeśli tylko jest taka możliwość.

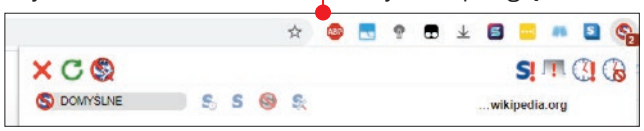


NOSCRIPT

Bardzo przydatny dodatek, którego zadaniem jest blokowanie skryptów JavaScript i apletów Java, Flash, Silverlight. Zapewnia to większe bezpieczeństwo, zwłaszcza jeśli odwiedzamy mało znane i potencjalnie niebezpieczne witryny, ponieważ blokada skryptów wykonywalnych chroni nas przed wyskakującymi oknami lub fałszywymi nakładkami na różnych witrynach.

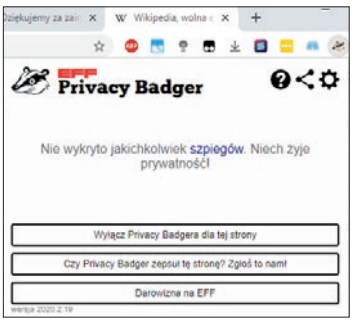
1 Po zainstalowaniu dodatku, by uzyskać do niego dostęp, należy kliknąć na jego ikonę na pasku adresowym przeglądarki.

2 W oknie ● możemy kontrolować, jakie elementy mogą być wyświetlane, a jakie mają być blokowane. Dzięki bardzo dobrej domyślnej konfiguracji właściwie nie trzeba zmieniać żadnych opcji, aby bezpiecznie korzystać z przeglądarki.



PRIVACY BADGER

Privacy Badger to dodatek jedyny w swoim rodzaju. Powstrzymuje wszelkie kody ze stron internetowych przed podpinaniem nam znacznika śledzącego. Taki znacznik pozwala firmom na tworzenie naszego profilu poprzez informacje uzyskane w wyniku śledzenia naszych wyszukiwań w sieci i odwiedzanych stron. Dodatek ten po wykryciu śledzącego kodu wyłącza go, a firma, która nas śledzi, otrzymuje informacje, że zniknęliśmy z sieci.
Privacy Badger dopiero po kilku sesjach z przeglądarką dostosuje swoje ustawienia i filtry do naszego trybu przeglądania. Możemy ręcznie wyłączać lub włączać elementy kontrolowane przez dodatek.



KOMUNIKATOR SIGNAL

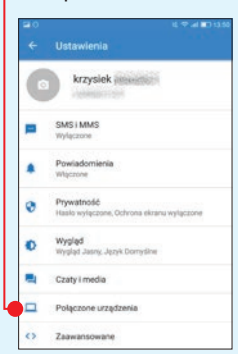
Android* iPhone*

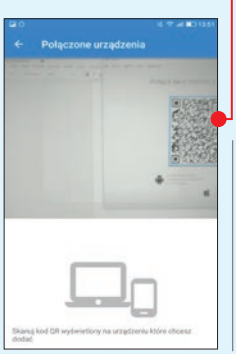
Signal (DVD-KOD: **099**) to dość nietypowy komunikator. Zanim zaczniemy w pełni z niego korzystać w środowisku Windows, wymagana jest jego instalacja na smartfonie. Potrzebny link w postaci kodu QR wyświetlony zostanie bezpośrednio w interfejsie programu. Po chwili konfiguracji będziemy mogli korzystać z bezpiecznego komunikatora na naszym komputerze. Signal pozwala na wysyłanie wiadomości tekstowych, obrazów, komunikację głosową, a nawet wideorozmowy. Cała komunikacja jest zabezpieczona i nikt nie będzie mógł nas podsłuchać ani sprawdzić, o czym piszemy. Dodatkowo możemy ustawić czyszczenie historii rozmów, dzięki czemu starsze wiadomości będą same znikały.

KONFIGURUJEMY PROGRAM DO PRACY

1 Zanim uruchomimy Signal na komputerze, musimy zainstalować go na naszym smartfonie, łatwo go znaleźć w sklepie z aplikacjami. Możemy skorzystać z kodów ●. Następnie uruchamiamy aplikację na smartfonie i postępujemy zgodnie z instrukcjami na ekranie.

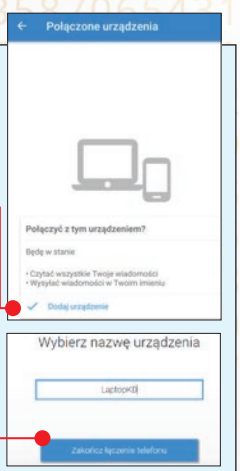
2 Dodajemy nasz komputer do aplikacji Signal. W smartfonie naciskamy kolejno **Ustawienia**, **Połączone urządzenia** ●, **+**. Uruchamiamy aplikację Signal na komputerze i skanujemy kod QR ● widoczny na ekranie komputera.





3 Naciskamy **Dodaj urządzenie** ● w smartfonie.

4 Na komputerze wprowadzamy nazwę urządzenia, z którego korzystamy, i klikamy na **Zakończ łączenie telefonu** ●.



5 Teraz będziemy mogli komunikować się ze znajomymi ●, wykorzystując nie tylko smartfon, ale i komputer, co może być wygodne podczas dłuższej pracy, a nasze dane będą bezpiecznie szyfrowane.

* Kod QR szybko przenosi na stronę, skąd można pobrać aplikację. W iPhonie skanujemy go aplikacją aparatu, użytkownicy Androida mogą użyć dowolnej aplikacji QR pobranej z Google Play

DLA ZAAWANSOWANYCH

ANONIMOWOŚĆ W INTERNECIE

Pozostanie anonimowym w sieci nie jest zadaniem najprostszym w realizacji. Obecnie praktycznie każdy ruch wykonywany w sieci jest rejestrowany i łatwo można wytropić użytkownika, który nie wie, jak się ukrywać. W tym poradniku przeczytamy, JAK SIĘ SKUTECZNIE UKRYĆ I ZACHOWAĆ ANONIMOWOŚĆ

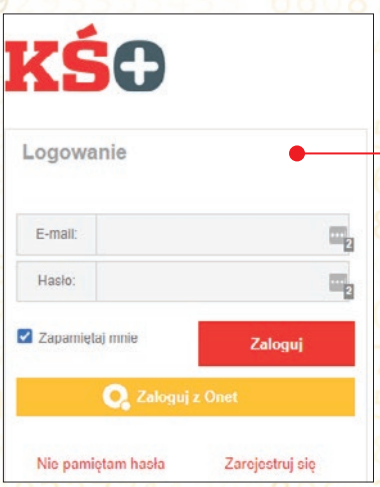
Coraz więcej osób jest świadomych tego, jak wiele informacji na ich temat jest dostępnych przez internet, właściwie można stwierdzić, że jesteśmy śledzeni na każdym kroku. Wszystkie odwiedzone przez nas strony, wyszukiwane przez nas hasła, przesyłane wiadomości, hasła, loginy – te i znacznie więcej informacji można przechwycić w ruchu sieciowym. Stwarza to duże zagrożenie, gdyż ktoś może wykorzystać uzyskane na nasz temat informacje w zły sposób. Oczywiście, z drugiej strony jeśli ktoś popełni przestępstwo przez internet, to dowody będą dostępne na przykład na serwerach ISP, czyli dostawcy internetu.

Korzystając z serwisów społecznościowych, właściwie sami zgadzamy się na pokazywanie naszego prywatnego życia publicznie. Wprawdzie możemy konfigurować opcje prywatności, jednak każda informacja, którą umieszczamy w takim serwisie, ma zasięg globalny i może zostać wykorzystana. Aktywne używanie tego typu usług jest zupełną przeciwnością prywatności i bezpieczeństwa w sieci.

Jeśli zależy nam na bezpiecznej komunikacji, na tym, by nasze wiadomości były szyfrowane i mogły być odczytane tylko przez nas i naszych odbiorców, powinniśmy wybierać komunikatory oferujące takie rozwiązania, a nie popularne czaty w aplikacjach społecznościowych.

JAK NIE DAĆ SIĘ ZDEMASKOWAĆ

Na kolejnych stronach poznamy metody pozwalające stać się anonimowym w sieci, głównie wykorzystując możliwości sieci TOR (więcej o tej sieci w dalszej części kursu). Jednak nawet korzystając z sieci umożliwiającej pełną anonimowość, możemy sami się zdradzić. Dlatego warto zapoznać się z kilkoma zasadami, których trzeba przestrzegać, aby pozostać anonimowym.

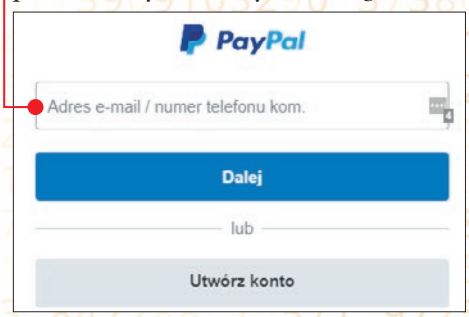


Nie logujemy się do wcześniej założonych kont, korzystając z sieci Tor

Z założenia każde konto zabezpieczone jest hasłem i wszystkie informacje dotyczące logowania zapisywane są na serwerze. Jeśli więc zalogujemy się na takie konto podczas korzystania z sieci Tor, będzie można powiązać nasz nowy adres IP z nazwą i danymi użytkownika danego konta.

Nie logujemy się przez sieć Tor na konta z dostępem do pieniędzy

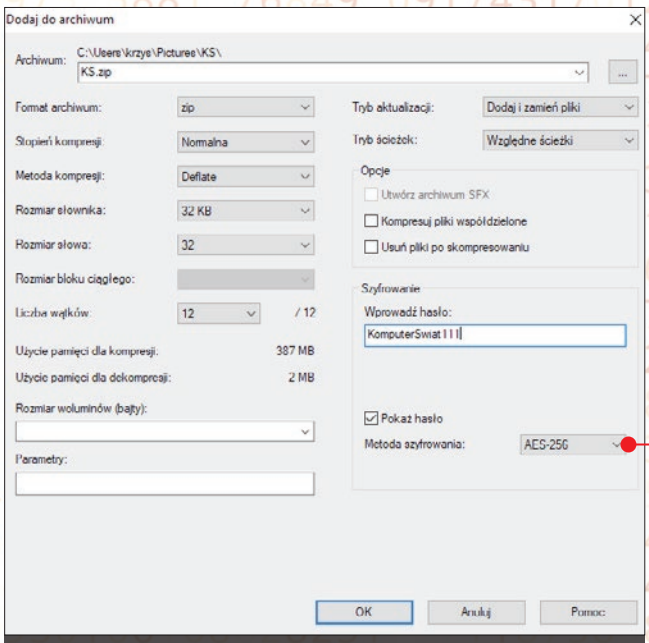
Musimy dać się odpowiednio zweryfikować, zanim otworzymy rachunek bankowy czy też potwierdzimy konto PayPal. Dlatego nie ma



sensu jednocześnie ukrywać swojej tożsamości w internecie i logować się do tego typu usług. Możemy również przysporzyć sobie kłopotów, ponieważ banki mogą blokować konta, do których następują logowania z różnych adresów IP w różnych krajach, by zabezpieczyć nas przed włamaniem.

Nie zmieniamy typu wykorzystywanej sieci w trakcie trwania jednej sesji

Jeśli korzystamy z sieci Tor przez na przykład 30 minut i stwierdzamy, że pracuje ona zbyt wolno, a potrzebujemy szybszego działania, choćby po to, by obejrzeć materiał wideo, nie otwieramy zwykłej przeglądarki i nie przeglądamy zasobów przy jednocześnie aktywnej przeglądarce Tor. Przez takie działanie bardzo łatwo powiązać adresy IP i czasy dostępu do serwerów. Powinniśmy całkowicie zamknąć przeglądarkę Tor i dopiero wtedy zacząć „normalnie" korzystać z internetu.



Korzystając z programu 7-Zip, wybierajmy metodę szyfrowania AES-256, która zapewnia wysoki poziom bezpieczeństwa

Nie przesyłamy wrażliwych danych bez ich zaszyfrowania

Nie wiemy, czy ktoś może nas szpiegować, ale wszelkie informacje, które są wrażliwe lub szczególnie ważne, nigdy nie powinny być przesyłane przez internet bez wcześniejszego zaszyfrowania. Jeśli nie zamierzamy korzystać ze specjalnych narzędzi do szyfrowania, powinniśmy przynajmniej spakować przesyłane pliki do archiwum i zabezpieczyć je hasłem. Nie jest to idealne rozwiązanie, ale szybkie i – jeśli ustawimy odpowiednio silne hasło – nie do złamania przez większość atakujących.

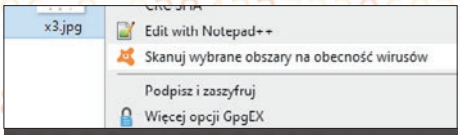
Nie otwieramy nieznanych linków i plików

Czasem trudno przewidzieć, czy otrzymany link otworzy prawdziwą stronę, czy jest to

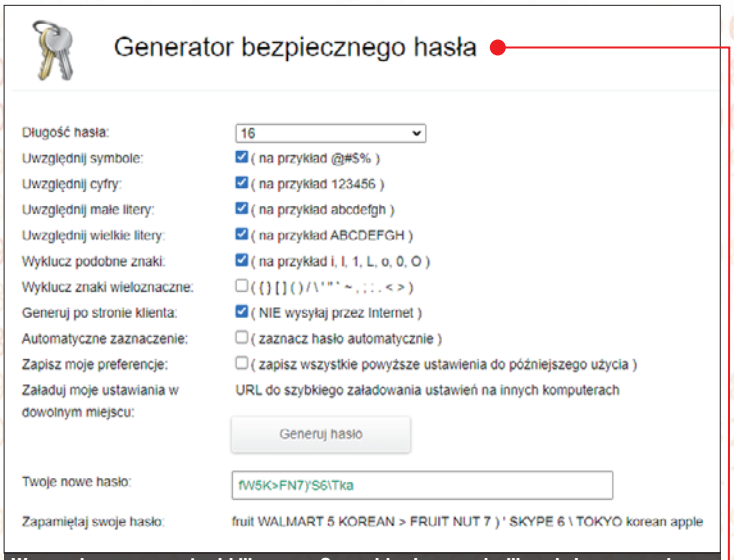
pułapka prowadząca do zainfekowanej witryny, która wykorzystując specjalne skrypty, przechwyci naszą przeglądarkę lub zainstaluje programy typu malware. Zagrożenie zawsze istnieje, gdy otwieramy nieznane pliki, które otrzymaliśmy drogą mailową lub sami pobraliśmy z podejrzanych stron. Wirusy mogą być ukryte nie tylko w aplikacjach, ale również w plikach muzycznych, zdjęciach, dokumentach. Jeżeli zależy nam na ochronie, powinniśmy zainstalować program antywirusowy, który ochroni nas przed tego typu zagrożeniami, jeśli już przypadkiem otworzyliśmy zły link. Większość programów AV pozwala na przeskanowanie pliku przed jego uruchomieniem. Wystarczy kliknąć na dany plik prawym przyciskiem myszy i wybrać z menu kontekstowego opcję Skanuj.

Nie podajemy wrażliwych danych online

Jeśli zależy nam na anonimowości, nie możemy podawać naszych danych na wielu stronach. Informacje typu wiek, data urodzenia, miejsce zamieszkania, ulubione zwierzę, drużyna, ksywa, hobby i inne tego typu informacje z pozoru wydają się mało szkodliwe. Jednak w większości przypadków, na przykład gdy chcemy odzyskać hasło do jakiejś usługi, musimy podać właśnie tego typu informacje. Jeżeli więc wcześniej podaliśmy w jakimś serwisie społecznościowym lub innym publicznym portalu tego typu informacje, atakujący mogą do nich dotrzeć i wykorzystać je przeciwko nam.



Większość programów antywirusowych pozwala na przeskanowanie pliku przed jego uruchomieniem. Wystarczy kliknąć na dany plik prawym przyciskiem myszy i wybrać z menu kontekstowego opcję Skanuj



Wprowadzamy parametry i klikamy na Generuj hasło – po chwili w oknie po prawej pojawią się losowe hasła, możemy wybrać jedno z nich i z niego korzystać

DBAMY O SILNE HASŁA

Bardzo dużo osób używa jako hasła swojego imienia i roku urodzenia lub nazwy drużyny piłkarskiej itp. Takie informacje można bardzo łatwo zebrać o każdej osobie i próbować złamać słabe hasło. Pamiętajmy, że musimy zabezpieczać nasze konta silnymi hasłami, które nie będą podatne na tego typu „społeczne" ataki. Silne hasło powinno mieć przynajmniej 12 znaków, na które składać się będzie przynajmniej 1 duża litera, cyfra i znak specjalny. Możemy korzystać ze specjalnych generatorów haseł jak na przykład generator online: **passwordsgenerator.net/pl**

CZYM JEST SIEĆ TOR

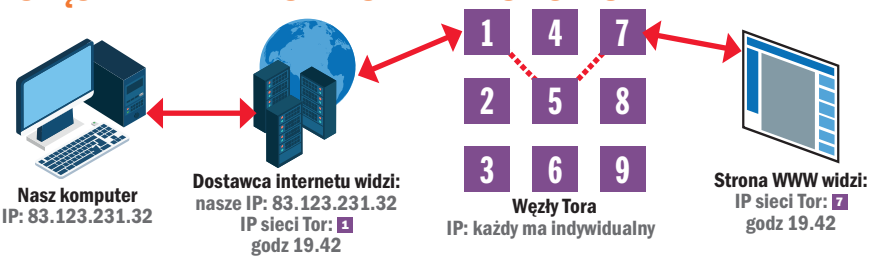
Tor to przykład sieci anonimowej, która podobnie jak inne, typu **Freenet**, **GNUnet** czy **MUTE**, ma za zadanie chronić naszą tożsamość w internecie. Głównym celem wykorzystywania takich sieci jest chęć ominięcia narzędzi cenzury, mechanizmów filtrowania sieci i różnego typu ograniczeń w komunikacji.

Sama sieć Tor oparta jest na zasadzie trasowania cebulowego. Nazwa tego mechanizmu bierze się stąd, że wykorzystując kryptografię, wielowarstwowo (stąd porównanie do cebuli) szyfrowane są wszystkie przesyłane komunikaty, które przesyłane są przez ciąg różnego typu serwerów – ruterów cebulowych, które nie mają informacji o danych, jakie przesyłają.

Każdy może wspomóc taką sieć, uruchamiając na swoim komputerze serwer, który będzie służył innym. Prosta implementacja, jasne zasady działania i możliwość praktycznie całkowitego zniknięcia w internecie to główne powody, dla których sieć Tor odniosła tak duży sukces.

W teorii możliwe jest wyśledzenie użytkownika i potwierdzenie komunikacji wychodzącej i przychodzącej do jego komputera, jednak wymaga to ogromnych środków i zaplecza technologicznego. Takie środki są stosowane w USA, gdzie rząd może kontrolować jednocześnie węzeł początkowy i końcowy, kluczowe dla całej komunikacji. Uważa się, że w przypadku innych państw potwierdzenie wystąpienia komunikacji jest praktycznie niemożliwe.

POŁĄCZENIE Z WYKORZYSTANIEM SIECI TOR



Gdy korzystamy z Tora, wybierana jest losowa trasa przez różne węzły sieci Tor. Dopiero ostatni węzeł odszyfrowuje nasz pakiet i wysyła go do właściwego serwera. Serwer nie wie, jaki jest nasz adres IP, a dostawca nie wie, z jakim serwerem się łączymy ani jakie dane przesyłamy

ETYKIETA KORZYSTANIA Z SIECI TOR

Bardzo ważne jest stosowanie się do kilku podstawowych zasad, które mają na celu zachowanie optymalnej wydajności poszczególnych routerów cebulowych dostarczanych przez ochotników i utrzymywanych na ich własny koszt. Za stosowanie etykiety powinniśmy sami brać odpowiedzialność, nikt nas nie ukarze, jeśli nie będziemy jej przestrzegać – jest to internetowy savoir-vivre, po prostu wypada go uwzględniać. Można wyróżnić trzy najważniejsze zasady.

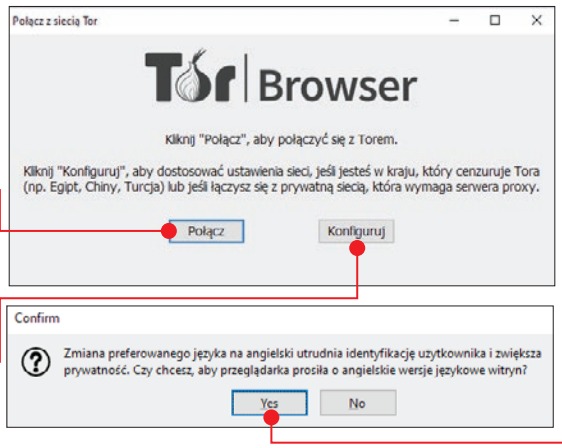
- **Nie należy obciążać sieci zbyt dużym transferem danych** – źle postrzegane jest przesyłanie bardzo dużej ilości danych przy wykorzystaniu sieci Tor, ponieważ w znacznym stopniu może wpłynąć to na obciążenie całej sieci i spowolnienie pracy innych użytkowników.
- **Nie należy korzystać z klientów torrent**– protokoły torrent nie powinny być wykorzystywane w sieci Tor, ponieważ przeważnie służą pobieraniu nielegalnych treści i dużej ilości danych, co generuje zbyt duży ruch w sieci. Dodatkowo domyślnie polityka węzłów wyjściowych blokuje standardowe porty klientów torrent.
- **Nie wolno rozsyłać spamu**– jego rozsyłanie jest domyślnie zablokowane na węzłach wyjściowych na porcie 25, rozsyłanie spamu z sieci Tor jest wysoce niestosowne.

Warto też mieć na uwadze, że serwisy i witryny internetowe mogą inaczej traktować internautów, których rozpoznają jako użytkowników sieci Tor. Przeważnie oznacza to ograniczenie przepustowości

Wyrwij, użyj dziurkacza i zbieraj do segregatora

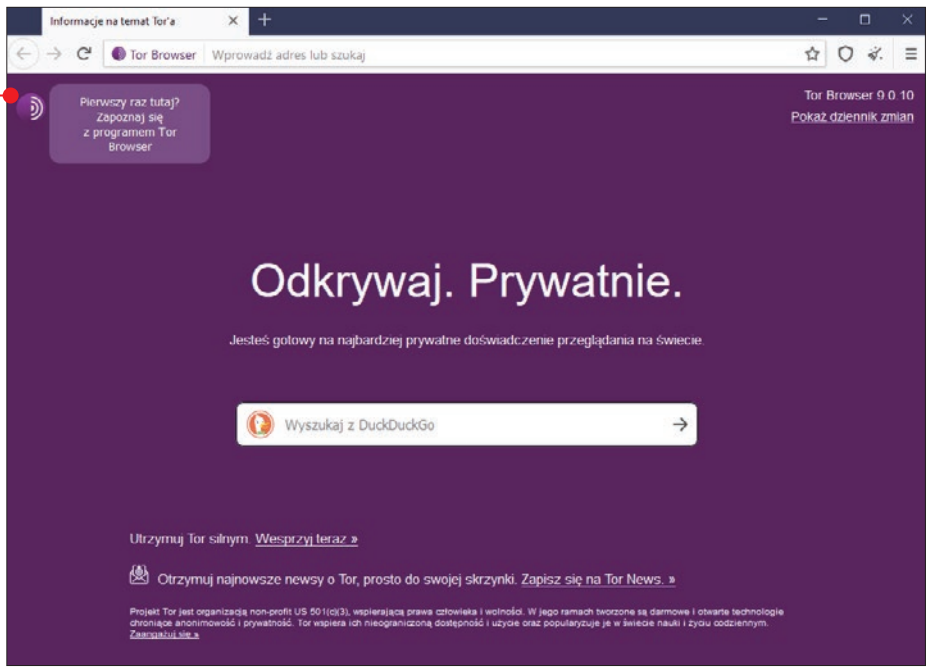
KORZYSTAMY Z PRZEGLĄDARKI TOR BROWSER W WINDOWS

Tor Browser możemy pobrać z KŚ+ (ksplus.pl), po jej zainstalowaniu i uruchomieniu musimy przeprowadzić krótką konfigurację.



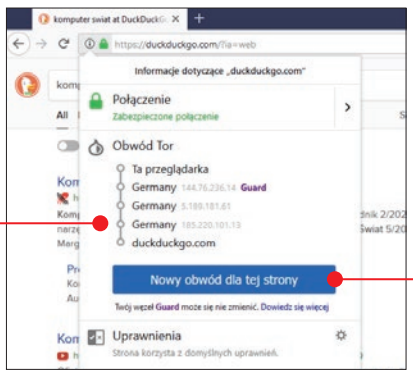
1 W pierwszym oknie klikamy na **Połącz**.

2 Po chwili powinno pojawić się okno przeglądarki z nawiązanym połączeniem (jeśli go nie zobaczymy, trzeba kliknąć w oknie z poprzedniego punktu na **Konfiguruj** i wprowadzić ustawienia serwera proxy, jeżeli z niego korzystamy).



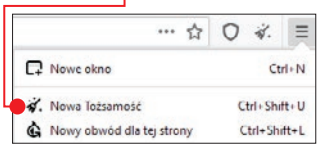
3 Przy próbie skorzystania z Tor Browser po raz pierwszy pojawi się alert związany ze zmianą języka wyszukiwania. Klikamy na **Yes** – dzięki temu trudniej będzie nas wykryć.

4 W każdej chwili możemy sprawdzić, że jesteśmy chronieni, klikając na symbol kłódki na pasku adresowym. Pojawią się wtedy szczegółowe informacje na temat utworzonego dla nas obwodu. Zawsze składa się on z minimum trzech węzłów. Na zewnątrz nasz adres IP jest widoczny jako adres ostatniego węzła.



5 Po kliknięciu na **Nowy obwód dla tej strony** zostanie zmieniony obwód jedynie dla danej witryny, a nie dla całej przeglądarki.

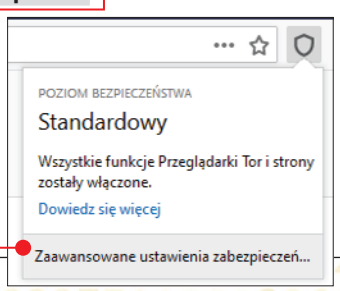
6 Jeśli chcemy uzyskać nowy obwód dla całej przeglądarki, należy kliknąć w prawym górnym rogu na trzy kreski, a następnie na **Nowa tożsamość**.



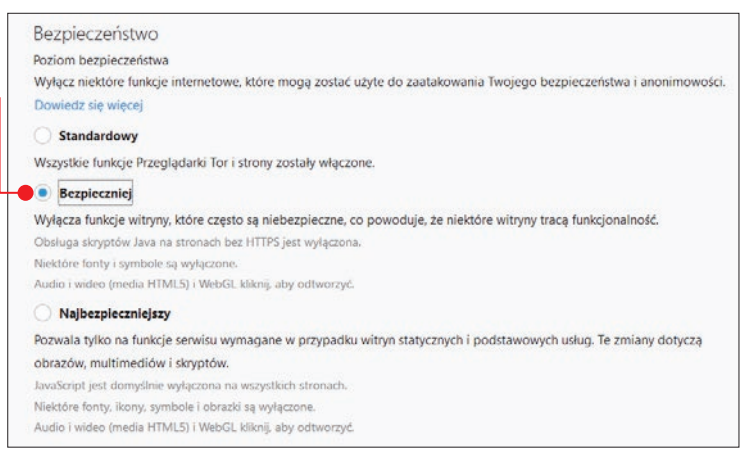
ZARZĄDZAMY USTAWIENIAMI BEZPIECZEŃSTWA

Tor Browser pozwala na skonfigurowanie poziomu zabezpieczeń w zależności od potrzeb użytkowników. Początkujący powinni zostawić wszelkie ustawienia w trybie domyślnym. Zaawansowanym użytkownikom zaleca się jednak dostosowanie ustawień do swoich wymagań.

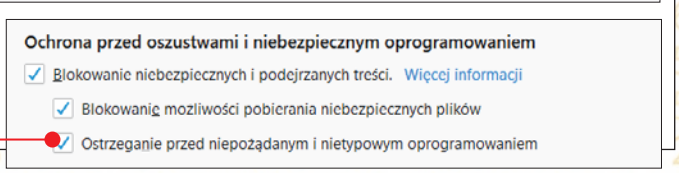
1 Klikamy na górnym pasku na ikonę tarczy, a następnie na **Zaawansowane ustawienia zabezpieczeń**.



2 Najlepiej wybrać profil **Bezpieczniej**, który pozwala w znacznym stopniu zabezpieczyć się dodatkowo w trakcie anonimowego surfowania w internecie.



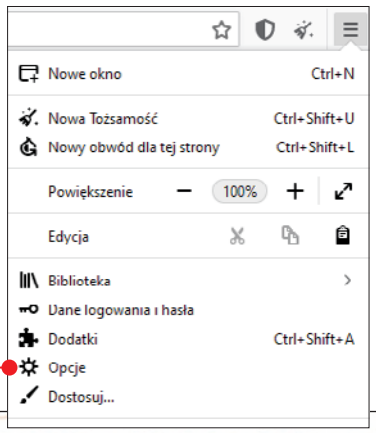
3 Dodatkowo zaleca się zaznaczenie wszystkich opcji w polu **Ochrona przed oszustwami i niebezpiecznym oprogramowaniem**.

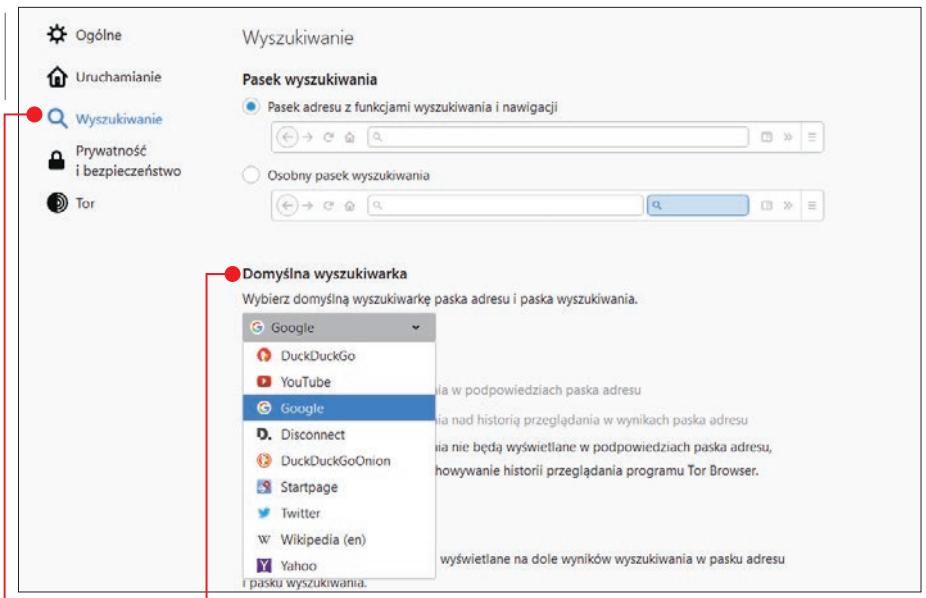


ZMIANA DOMYŚLNEJ WYSZUKIWARKI

W Tor Browser domyślną wyszukiwarką jest **DuckDuckGo**. Jeśli chcemy, możemy zmienić domyślny silnik wyszukiwania. Nawet korzystanie z silnika Google nie będzie zagrażało naszej anonimowości, gdyż będziemy używać zupełnie innego adresu IP.

1 Klikamy na trzy kreski w prawym górnym rogu okna, a następnie na **Opcje**.

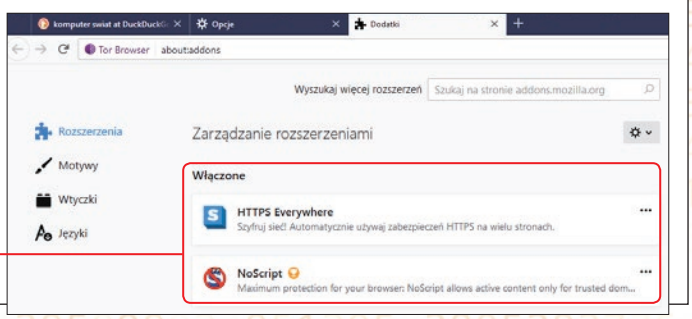




2 Teraz po lewej stronie klikamy na **Wyszukiwanie**, a po prawej z listy w sekcji **Domyślna wyszukiwarka** wybieramy taką wyszukiwarkę, która nam odpowiada.

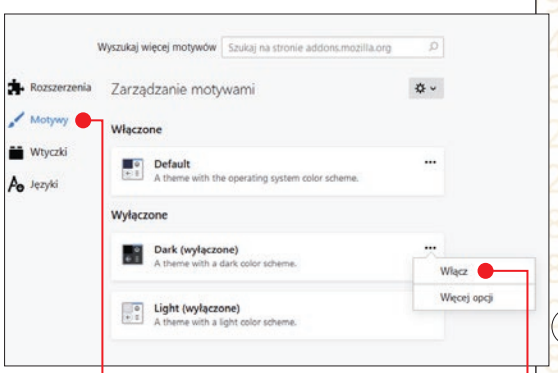
BEZPIECZNE DODATKI

Tor Browser także tak jak inne przeglądarki może korzystać z dodatków, które dodatkowo dbają o nasze bezpieczeństwo – **HTTPS Everywhere** oraz **NoScript**. Dodatki możemy zainstalować, korzystając ze sklepu Mozilli. **Uwaga!** W Tor Browser instalujmy tylko i wyłącznie takie dodatki, co do których jesteśmy absolutnie pewni, że w tle nie wysyłają one danych o naszym systemie i nie naruszają naszej anonimowości.



ZMIANA MOTYWU PRZEGLĄDARKI

Domyślnie Tor Browser działa z jasnym motywem graficznym. Dostępny jest jednak także ciemny motyw. Oto jak szybko go ustawić.



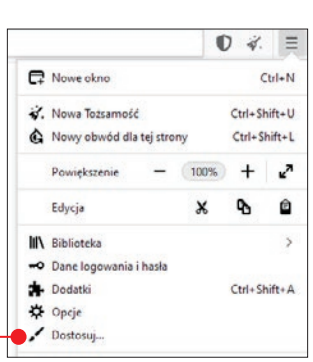
1 W głównym oknie klikamy na trzy kreski w prawym górnym rogu, a potem na **Dodatki**.

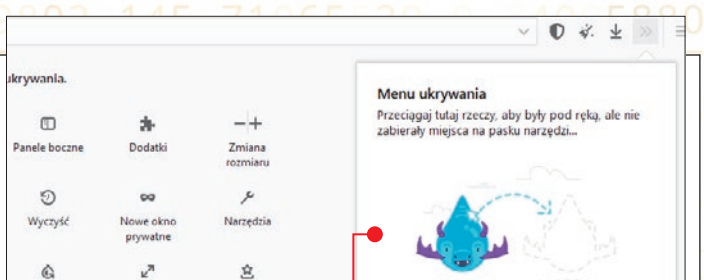
2 Po lewej klikamy na **Motywy**, a po prawej przy motywie **Dark** na trzy kropki i na **Włącz**.

MENU UKRYWANIA

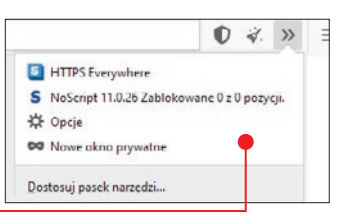
W najnowszej wersji przeglądarki Tor Browser dodano funkcję **Menu ukrywania**. Pozwala ona na dodanie do górnego paska naszych ulubionych skrótów, dzięki czemu zawsze będziemy mieli je pod ręką.

1 W głównym oknie programu klikamy na trzy kreski w prawym górnym rogu, a następnie na **Dostosuj**.





2 Teraz możemy przeciągnąć wybrane elementy w obszar menu ukrywania.



3 Dzięki temu będą zawsze pod ręką – jednak nieco ukryte.

Wyrwij, użyj dziurkacza i zbieraj do segregatora

TAILS ANONIMOWY SYSTEM OPERACYJNY

Tails pozwoli nam zachować anonimowość w internecie. NARZĘDZIA I MECHANIZMY WBUDOWANE W TEN SYSTEM CHRONIĄ PRZED ZDRADZENIEM TOŻSAMOŚCI JEGO UŻYTKOWNIKA PODCZAS KORZYSTANIA Z SIECI. W tym odcinku kursu przeczytamy, jak korzystać z Tailsa i poznamy jego funkcje

Czym właściwie jest Tails? Jest to system operacyjny oparty na środowisku Linux, którego głównym zadaniem jest sprawienie, aby korzystający z niego użytkownik stał się anonimowy w internecie.

Nazwa **TAILS** to akronim od **The Amnesic Incognito Live System**, co można przetłumaczyć jako „system w wersji na żywo zapewniający amnezję". Chodzi o to, że dane użytkownika i informacje o odwiedzanych witrynach nie są przechowywane, ale zapominane.

Jak sama nazwa wskazuje, system jest stworzony do działania w wersji Live, czyli bez instalacji. Jest za każdym razem doraźnie uruchamiany ze swojego nośnika – z płyty czy pendrive'a. Używając go, możemy pobierać pliki z internetu lub sami tworzyć dokumenty, jednak domyślnie są one przechowywane jedynie w pamięci podręcznej – do czasu wyłączenia systemu. Po zakończeniu pracy z Tailsem wszystkie dane zostają utracone. Rozwiązanie to ma służyć zapewnieniu prywatności i bezpieczeństwa użytkownikowi – po wyjęciu nośnika z systemem na komputerze nie zostają żadne ślady.

Jeżeli jednak potrzebujemy stałej przestrzeni dyskowej, by zapisywać na niej dane, nad którymi pracujemy, możemy skorzystać ze specjalnego trybu **persistence**. Pozwala on utworzyć na nośniku USB, na którym znajduje się Tails, specjalne miejsce na pliki – wtedy możemy je zapisywać tak, jakbyśmy korzystali z tradycyjnego systemu operacyjnego. Rozwiązanie to pozwala także aktualizować Tailsa.

Innym sposobem na zachowywanie danych jest zapisywanie ich na dodatkowym nośniku przenośnym lub w bezpiecznej chmurze.

Tailsa można umieścić na DVD lub na pendrivie. To drugie rozwiązanie jest wygodniejsze – system uruchamiany z USB działa sprawniej niż z płyty i mamy możliwość utworzenia specjalnej przestrzeni na dane (tryb **persistence**).

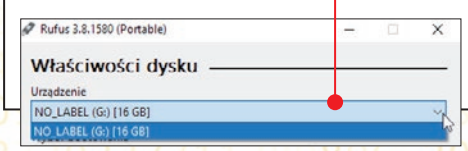
TWORZYMY BOOTOWALNY NOŚNIK USB Z SYSTEMEM TAILS

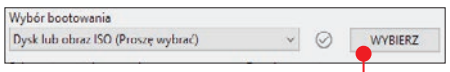
Na płycie dołączonej do Niezbędnika znajduje się obraz ISO **Tailsa** (w **KŚ+**). Korzystając z niego i z programu **Rufus** (DVD-KOD: **064**), utworzymy bootowalny nośnik USB. Umieszczając Tailsa na pendrivie, będziemy mogli nie tylko korzystać z anonimowego systemu, ale też aktualizować go i zapisywać pliki, nad którymi pracujemy. A jeśli skorzystamy z bardzo wydajnego nośnika typu USB 3.0, może się okazać, że system w wersji Live będzie pracował równie wydajnie jak system na dysku twardym. **Uwaga!** Pendrive powinien mieć przynajmniej 8 GB pojemności i nie może zawierać ważnych danych – zostaną one utracone.

1 Kopiujemy na dysk z płyty DVD lub pobieramy z **KŚ+** plik ISO z systemem Tails – **tails-amd64-4.8.iso**

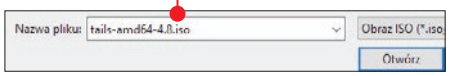
2 Następnie uruchamiamy program **Rufus**, który umożliwia tworzenie bootowalnych nośników.

3 Umieszczamy nośnik USB w komputerze, na górze okna Rufusa powinniśmy zobaczyć nazwę wykrytego pendive'a. W razie potrzeby wybieramy go z listy.



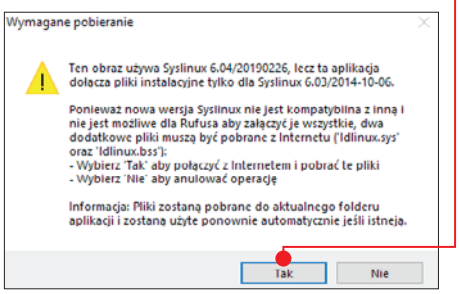


4 Następnie klikamy na **Wybierz**, wskazujemy obraz ISO systemu Tails i klikamy na **Otwórz**.

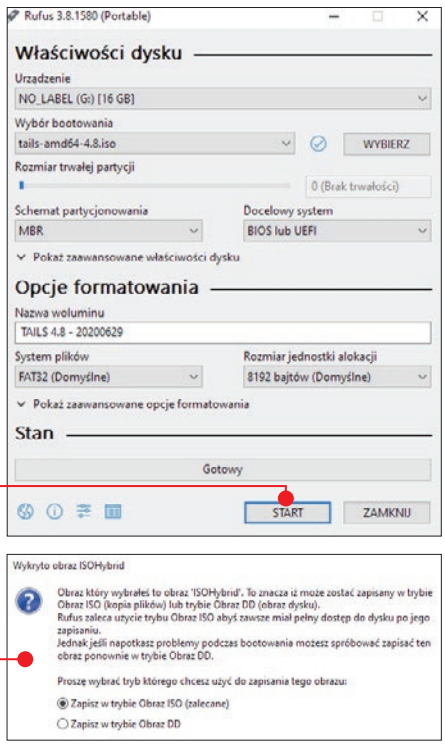


5 Na dole okna programu pojawi się aktualnie załadowany obraz, wystarczy teraz kliknąć na **Start**.

6 Następnie musimy kliknąć na **Tak**, żeby pobrać dodatkowe aktualne pliki instalacyjne.



7 Teraz pojawi się okno z informacją o obrazie ISO Hybrid – pozostawiamy domyślne ustawienia i klikamy na **OK**.

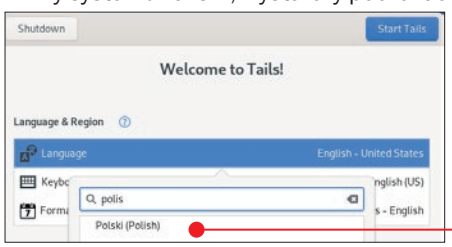


8 Potwierdzamy zgodę na formatowanie nośnika. **Uwaga!** Wszelkie dane z pendrive'a zostaną nieodwracalnie usunięte. Po chwili bootowalny nośnik będzie gotowy.

PIERWSZE URUCHOMIENIE TAILSA

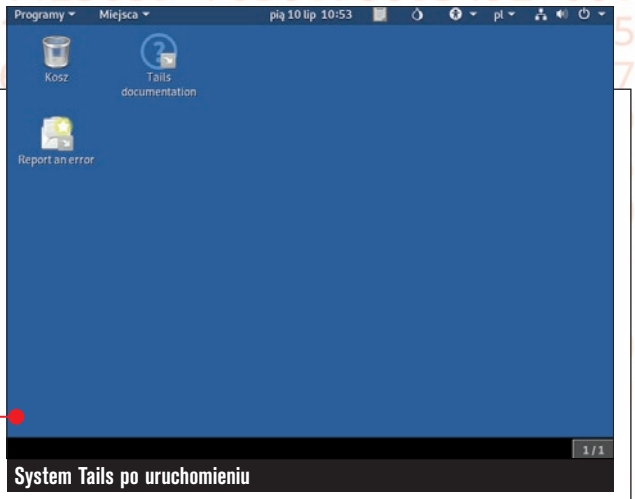
1 Podłączamy bootowalny nośnik do komputera. Uruchamiamy komputer i w czasie startu przechodzimy do ustawień BIOS-u lub Boot Menu (najczęściej trzeba wcisnąć klawisze F2, F8, F10 lub delete – odpowiednia informacja powinna być widoczna na ekranie). Wskazujemy nośnik z Tailsem jako ten, z którego ma wystartować komputer.

2 Teraz powinniśmy zobaczyć ekran startowy systemu Tails, wystarczy poczekać trzy sekundy lub nacisnąć klawisz enter.

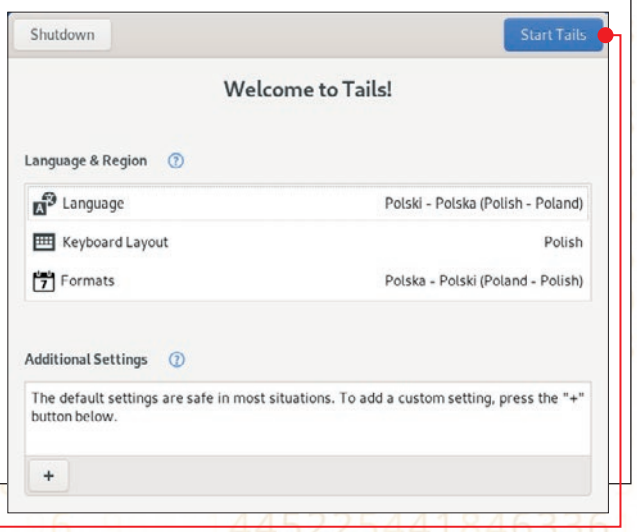


3 Pojawi się okno logowania do systemu. Zanim przejdziemy dalej, klikamy na **Language** na środku ekranu i wybieramy z listy **Polski (Polish)**.

4 Teraz możemy przejść do systemu, klikając na **Start Tails**. Oto pulpit Tailsa.

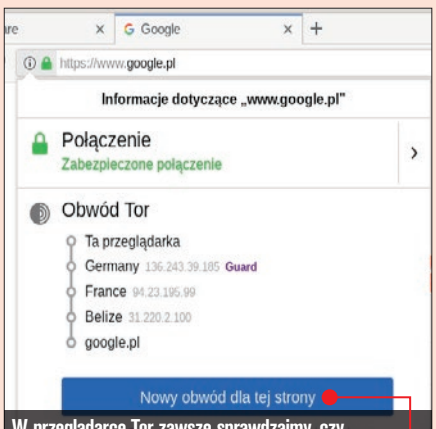


System Tails po uruchomieniu



Tails i anonimowość

Cały system operacyjny Tails został tak opracowany, aby domyślnie zapewnić użytkownikowi anonimowy dostęp do internetu i chronić prywatność. Jednak – podobnie jak w wypadku sieci Tor – jeżeli sami nie będziemy przestrzegać zasad bezpieczeństwa, będzie można nas zdemaskować. Dlatego nie należy logować się na konta, z których korzystaliśmy wcześniej, bez Tailsa. Nie wolno także korzystać z wątpliwych, nieznanych nam aplikacji czy serwisów, bo mogą narazić nas na wyciek danych. I oczywiście, jeśli chcemy pozostać anonimowi, nie powinniśmy wykonywać działań, które pozwalają nas zidentyfikować, jak logowanie się do kont bankowych czy udostępnianie zdjęć czy informacji o nas w internecie. Nie należy także korzystać z Tailsa w otwartych sieciach Wi-Fi ani przesyłać wrażliwych danych bez szyfrowania.

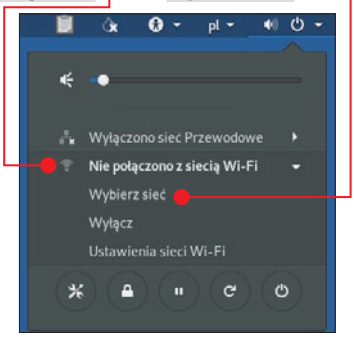


W przeglądarce Tor zawsze sprawdzajmy, czy połączenie z witryną jest bezpieczne i czy obwód ma trzy węzły i jest skonfigurowany. W każdej chwili możemy zmienić tożsamość w sieci, klikając na

ŁĄCZYMY SIĘ Z INTERNETEM

Jeśli korzystamy z połączenia przewodowego z internetem, wystarczy podłączyć przewód do komputera, a system automatycznie powinien skonfigurować połączenie i uzyskać dostęp do sieci. W przypadku gdy chcemy połączyć się z siecią Wi-Fi, musimy wykonać kilka prostych kroków.

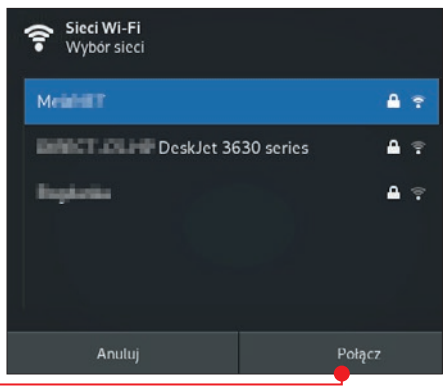
1 Klikamy w górnym prawym rogu na strzałkę, a następnie na **Nie połączono z siecią Wi-Fi** i na **Wybierz sieć**.

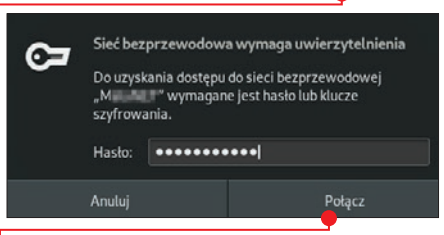


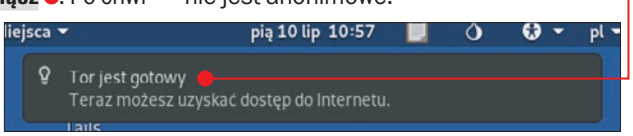
2 Teraz klikamy na sieć, z którą chcemy nawiązać połączenie, i na **Połącz**.

3 Następnie podajemy hasło dostępu do sieci Wi-Fi i klikamy na **Połącz**. Po chwili połączenie z siecią zostanie nawiązane i będziemy mieli dostęp do internetu. Po połączeniu z internetem automatycznie zostanie nawiązane połączenie z siecią Tor, która zapewni nam anonimowość.

Uwaga! Jeśli w trakcie pracy pojawi się na górnym pasku przekreślona ikona cebuli, oznaczać będzie to, że nasze połączenie nie jest anonimowe.



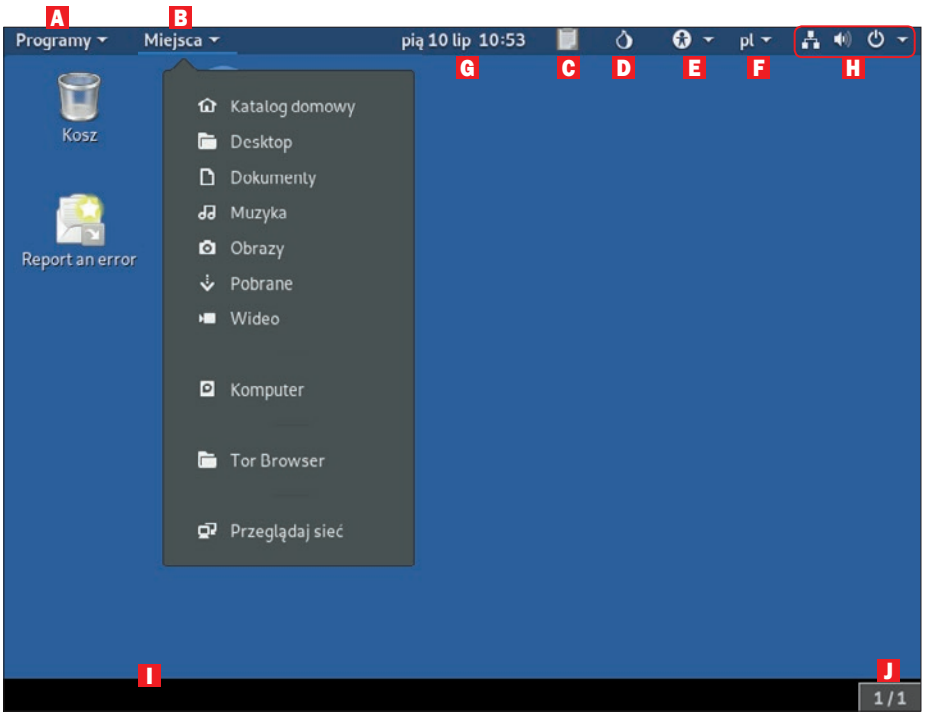




Wyrwij, użyj dziurkacza i zbieraj do segregatora

KORZYSTAMY Z SYSTEMU

Interfejs systemu jest dość prosty w obsłudze. Osoby korzystające na co dzień z Windows nie powinny mieć większych problemów z obsługą Tailsa.

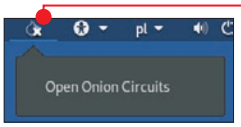


A Programy – lista z wszystkimi aplikacjami podzielonymi na kategorie

B Miejsca – dostęp do najważniejszych katalogów w systemie

C Schowek – przechowywanie skopiowanych treści

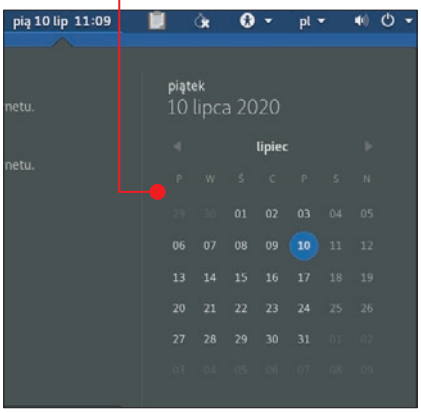
D Open Onion Circuits – informacje o dostępnych węzłach sieci Tor, **x** obok symbolu oznacza brak łączności z bezpieczną siecią.



E Ułatwienia dostępu

F Wybór języka i klawiatury

G Kalendarz z zegarem

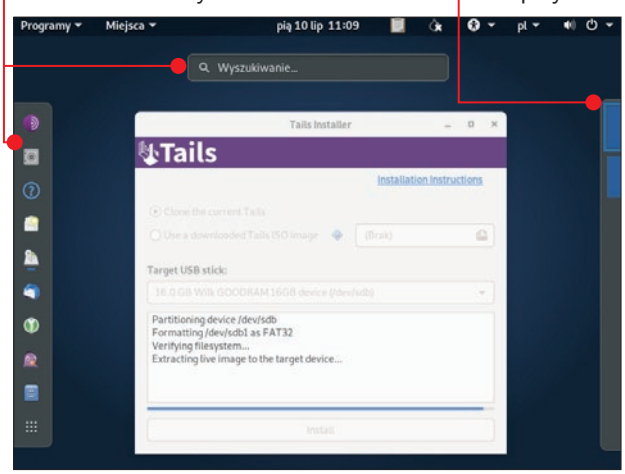


H Połączenia sieciowe, dźwięk i wyłączanie systemu

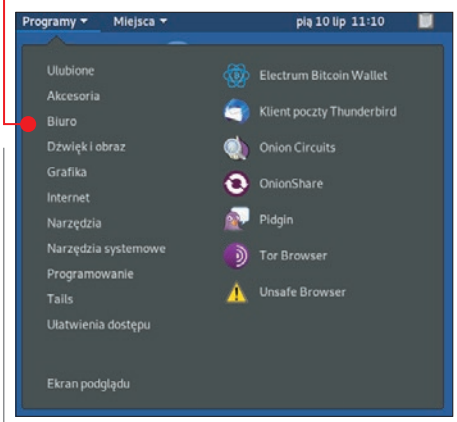
I Pasek zadań z aktywnymi programami

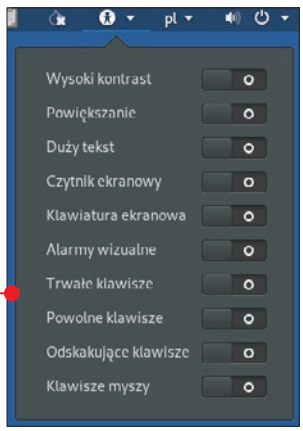
J Wybieranie **obszarów roboczych**

Dodatkowo jeśli przesuniemy kursor w skrajny lewy róg lub wciśniemy klawisz ⊞ – otworzy się specjalny launcher znany z systemu Debian. Pomaga on szybko znajdować potrzebne programy. A po prawej stronie wysuwa się pasek do zarządzania obszarami roboczymi.



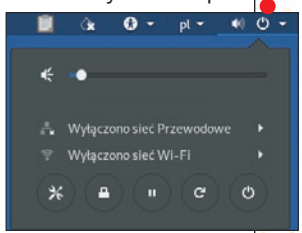
Jeśli klikniemy na **Programy**, otworzy się lista wszystkich programów dostępnych w systemie, podzielonych na kategorie według zastosowania. Najważniejszy z programów znajduje się w kategorii **Internet** i jest to przeglądarka **Tor Browser** – to ona zapewni nam anonimowość w sieci.





Opcje ułatwień dostępu są bardzo pomocne. Na przykład funkcja klawiatury ekranowej przyda się zawsze wtedy, gdy będziemy musieli podać dane dostępowe – jest bezpieczniejsza niż klawiatura fizyczna. Wystarczy aktywować odpowiednią opcję w menu ułatwień dostępu.

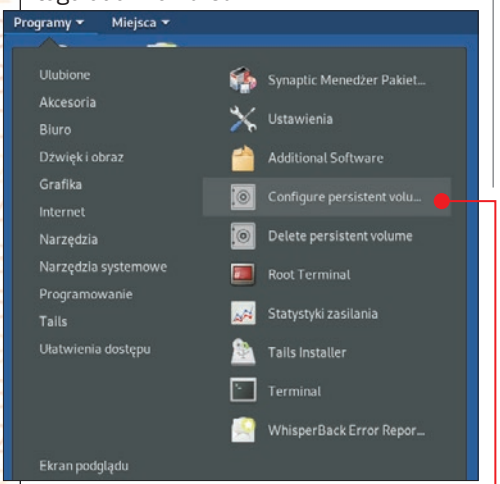
Klikając w skrajnym prawym rogu okna, wysuniemy aplet zarządzania systemem. Z jego poziomu szybko przejdziemy do ustawień systemu, ustawień sieciowych, skonfigurujemy ustawienia dźwiękowe i wyłączymy lub zablokujemy system. Przy wyłączaniu Tails zawsze zaciera wszelkie ślady, jakie mogliśmy zostawić. Wykonywane jest nawet czyszczenie pamięci RAM. Dlatego warto zamykać poprawnie system, aby uniknąć pozostawienia jakichkolwiek oznak korzystania z komputera.



TWORZYMY ZASZYFROWANĄ PARTYCJĘ NA DANE UŻYTKOWNIKA

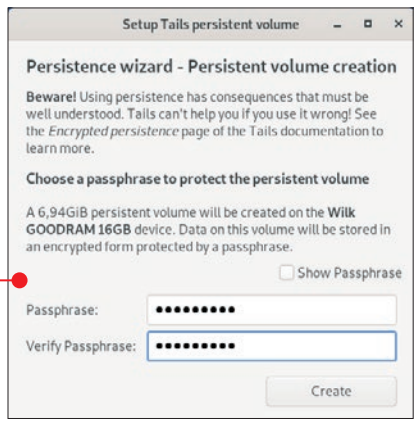
Tails umożliwia nam skonfigurowanie specjalnej przestrzeni dyskowej o nazwie **persistent volume**, zabezpieczonej hasłem, na której będziemy mogli przechowywać nasze pliki. Dodatkowo dzięki temu rozwiązaniu będziemy mogli łatwiej korzystać z takich funkcji systemu, jak na przykład szyfrowanie wiadomości, do czego potrzeba w pełni skonfigurowanego, zainstalowanego lokalnie, klienta poczty. Po utworzeniu tej specjalnej dodatkowej przestrzeni dyskowej będziemy mieli możliwość przechowywania również plików konfiguracyjnych, czyli zapisywania zmian wprowadzanych w systemie.
Uwaga! Ta opcja jest możliwa do skonfigurowania tylko w przypadku korzystania z nośnika USB z zainstalowanym systemem Tails.

1 Musimy utworzyć bootowalny nośnik USB z systemem Tails jak na pierwszej stronie tego odcinka kursu.



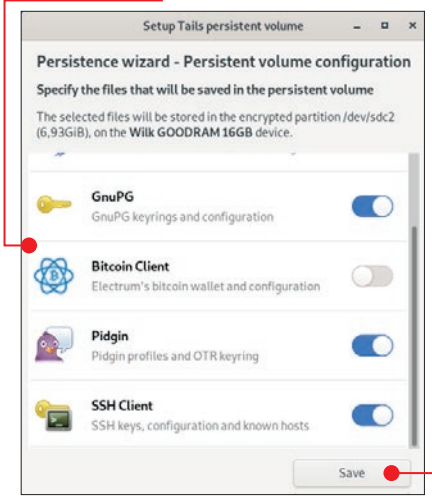
2 Uruchamiamy system Tails i przechodzimy do pulpitu.

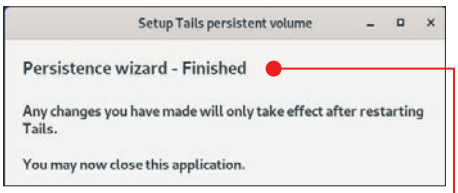
3 Klikamy w górnym lewym rogu na **Programy**, najeżdżamy kursorem na **Narzędzia systemowe** i klikamy na **Configure persistent volume**.



4 Uruchomiony zostanie kreator przechowywania danych. Na pierwszym ekranie podajemy hasło, które będzie służyło do ochrony naszych danych. Klikamy na **Create**. W wypadku przykładowego nośnika o rozmiarze 16 GB można wykorzystać tylko 6,94 GB jako miejsce na dane użytkownika.

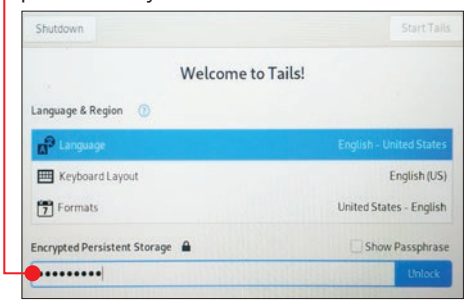
5 Na następnym ekranie zaznaczamy, z jakich opcji chcemy korzystać i jakie pliki będą mogły być przechowywane w nowo utworzonej przestrzeni. Po wybraniu odpowiednich opcji klikamy na **Save**.





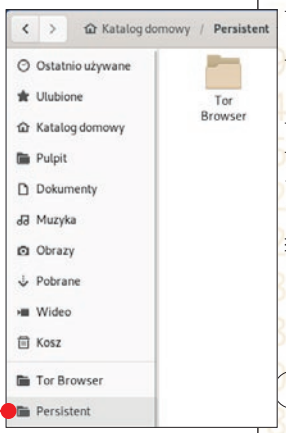
6 Gdy zobaczymy okno z informacją o zakończeniu działania kreatora, zamykamy go i ponownie uruchamiamy system Tails.

7 Przy ponownym uruchomieniu komputera wystarczy na ekranie logowania systemu Tails w polu **Encrypted Persistent Storage** podać nasze hasło (z punktu **4**) i kliknąć na **Unlock**. Jeśli wpisane hasło jest poprawne, przestrzeń dyskowa zostanie odblokowana.



8 Klikamy na **Start Tails** i zaczynamy korzystanie z systemu i naszej przestrzeni na dane.

9 Dostęp do niej uzyskamy, klikając na pulpicie na **Katalog domowy** i na **Persistent**. Wszystkie pliki w tym katalogu będą zaszyfrowane i nie będą automatycznie usuwane przy kolejnych uruchomieniach systemu.

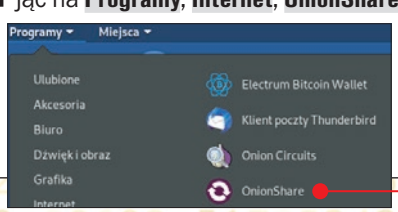


Wyrwij, użyj dziurkacza i zbieraj do segregatora

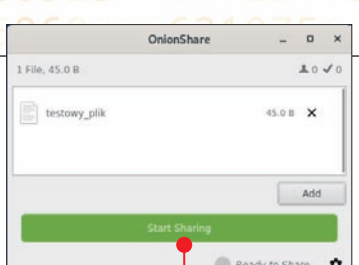
ONIONSHARE

Jest to specjalna aplikacja, która pozwala na anonimowe przesyłanie plików, korzystając z sieci Tor. Nasz odbiorca nie musi mieć zainstalowanego programu **OnionShare** (DVD-KOD: **060**), wystarczy przeglądarka Tor Browser.

1 Uruchamiamy program OnionShare, klikając na **Programy**, **Internet**, **OnionShare**.

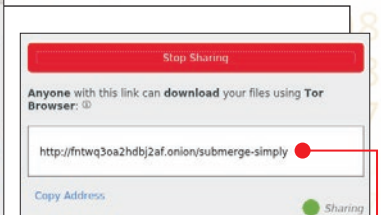
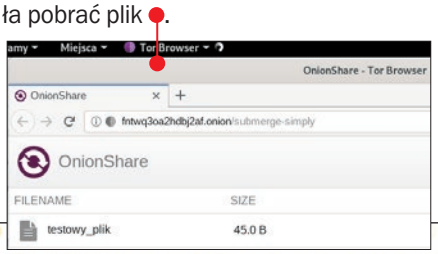


2 Przeciągamy na okno programu plik lub folder, który chcemy przesłać, alternatywnie możemy kliknąć na **Add Files** lub **Add Folder**.



3 Aby rozpocząć przesyłanie pliku, klikamy na **Start Sharing**.

4 Kiedy plik będzie gotowy do udostępnienia, pojawi się „zielone światło". Wtedy należy przekazać w bezpieczny sposób link osobie, której chcemy przesłać plik.



5 Wystarczy, że osoba ta otworzy link za pomocą przeglądarki Tor, a będzie mogła pobrać plik.